UNIVERSITY OF OSLO
Department of Informatics

Digital Subthreshold CMOS

Sequencing and Logic Elements for Power Analysis Resistance

Master thesis

Håvard Pedersen Alstad

2nd May 2008

Abstract

This thesis examines subthreshold operation for reducing power consumption and protection against power analysis attacks of digital CMOS circuits. Subthreshold operation is considered the most efficient way to reduce the power consumption of CMOS.

There are few studies analyzing the performance of sequencing elements in subthreshold region. Sequencing elements play an important part of clocked sequential circuit systems.Therefore, it is necessary to have a good understanding of the different design types and their applicability in subthreshold circuits.

In this thesis, different flip-flop designs commonly used in superthreshold systems are compared in subthreshold operation. According to process corner simulations, a PowerPC 603 type flip-flop operates successfully in all corners in a 65 nm process down to a power supply voltage of 125 mV. This flip-flop has a delay time of 28.7 ns and a power consumption of 2.4 nW in the typical corner. The power consumption decrease corresponds to a reduction factor of 20 000, compared to normal operation.

As cryptographic algorithms have become more secure against cryptoanalysis attack, several types of attacks exploiting physical emitted informations have been reported. Power analysis attacks use the power consumption pattern to attack the chip. An increasing demand for secure data communication makes it even more important to design with resistance against side channel attacks in mind for certain applications.

Operating in subthreshold region significantly reduces the signal amplitude and the dynamic power consumption component. The reduction of these elements is used to create a S-box for the AES encryption cipher with increased resistance against power analysis attacks. By running with subthreshold operation, the correlation between power consumption of different input values decreases with a factor of 2 500 at the cost of 350 times delay degradation.

Simulations in 90 nm and 65 nm processes provided by STMicroelectronics are performed in Cadence Virtuoso Platform.

Abstract

Preface

This thesis is submitted as part of the degree *Master of Informatics* in Microelectronics at the Department of Informatics, University of Oslo. The project was initiated in November 2006 and concluded in May 2008.

The work on this thesis has been very interesting and challenging in many ways. The thesis addresses several relatively new topics in the VLSI design area, which in recent years have gained increased interest in research and development. Among other things, the project has lead to four scientific publications. Through the work on this project, I got the opportunity to participate on the Design and Diagnostics of Electronic Circuit Systems 2008 conference in Bratislava, Slovakia. The conference was both interesting and inspiring.

First of all, I would like to thank my supervisor Snorre Aunet for accepting me as his student and for inspiration and guidance during this project. Helpful discussions have driven the project forward and given valuable inputs on the work.

I want to thank the students at the laboratory, especially Trygve, Svein, Kristin, Olav, Jan Erik, Bård, Daniel, Kristian, Elias, Henning, Jostein, Håkon O. and Nikolaj for interesting discussions of both relevant and non-relevant contents and breaks during long working days. Thanks to Håkon H. and Hans for help and guidance on technical matters. I would also like to thank the rest of the students and staff at the Nanoelectronic research group.

Lastly, I would thank my family for support during the project.

Oslo, May 2008

Håvard Pedersen Alstad

Contents

Chapter 1

Introduction

Techniques for reducing the power consumptions in power-hungry Very Large Scale Integrated Circuit (VLSI) systems are presently becoming a major challenge and obstacle for future development of Complementary Metal-Oxide Semiconductor (CMOS) technology. The International Roadmap for Semiconductors states that power management is now the primary issue across most application segments [1]. In a 45 nm CMOS process, you can fit more than 2000 transistors across the width of a human hair [2]. When all transistors switch billions of times per second they consume an enormous amount of energy compared to the area, which is dissipated as heat.

Moore presented in 1965 a prediction of further downscaling of Integrated Circuit (IC) technology by doubling the transistor density every 18 months [3]. Fig. 1.1 illustrates the exponential increase in transistor count in Intel ®Processors over the last 37 years. The increased packing density has been accompanied with increased speed, and has lead to an enormous increase in heat generation. The total chip performance is limited by the thermal dissipation capability of the mounted IC package of many of today's circuits [4].

With further downscaling of CMOS technology into deep submicron region even more transistors will be squeezed into an even smaller area. Power consumption in CMOS devices must be reduced to allow further development.

Another recent topic of interest, with the increased demand for secure communication presently is side-channel attacks. A cryptographic cipher implemented in an IC produces variation in power consumption and electromagnetic radiation due to switching activity of transistors. These variations are easily measurable with physical access to the IC and may be used to extract internal information from the circuit. With increased strengthening of cryptographic algorithms against cryptoanalysis, several types of attacks exploiting this physical emitted information have been

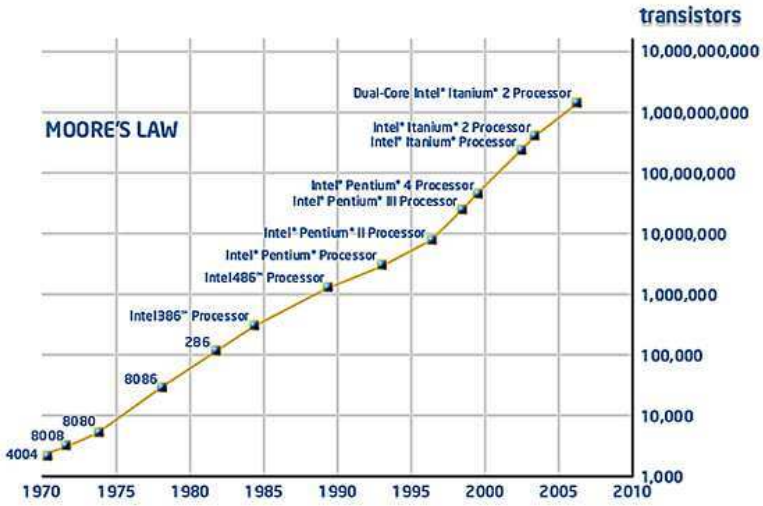


Figure 1.1: Moore's law Microprocessor Chart. Intel ®Corporation 2007

reported (e.g. [5, 6, 7]). Physical attacks on the implementation of the circuit, exploiting physical measurable information emitted by the device are referred to as side-channel attacks.

Side-channel attacks have become a major security threat to implementation of modern cryptographic ciphers immune to cryptoanalysis attacks. An increasing demand for secure data communication makes it more important to design with protection against side-channel attacks in mind for certain applications. Attacks on modern cryptographic ciphers have been reported to extract the correct 128 bit secret key within 3 minutes [8].

This thesis addresses both the performance of sequencing elements in the subthreshold region and techniques for improving the resistance against power analysis attacks with subthreshold operation in 4 papers included in the thesis.

1.1 Motivation

Power consumption management is becoming of primary concern in the design of modern IC. Subthreshold operation is attained by reducing the operating voltage of the chip below the transistors threshold voltage. Reducing the power supply voltage is regarded as the most direct and dramatic means of reducing power consumption [9]. Subthreshold operation results in huge decrease of power consumption at the expense of decreased maximum switching frequency. Operating CMOS circuits in their subthreshold region is a promising method for reducing the power dissipation of ultra-low-power-application.

Few studies have been done on performance of sequencing elements in the subthreshold region. As sequencing elements play an important part of clocked sequential circuit systems, it is important to have a good understanding of which type of design to choose in different applications in a subthreshold CMOS system. In this thesis different flip-flop designs commonly used in superthreshold systems are compared in subthreshold operation. The comparison is done with respect to delay time, power consumption, Power-Delay Product and Energy-Delay Product. Process corner performance is also simulated.

Increased resistance against power analysis attacks is obtained by reducing the signal magnitude [5]. Subthreshold operation reduces the signal amplitude significantly and can be used to increase resistance against side-channel attacks by reducing the power consumption. Reducing the signal amplitude by reducing the supply voltage makes it harder to measure the variation in power consumption. Normal arithmetic functions and a cryptographic function, the Advanced Encryption Standard (AES) S-box operation, are tested for improved power analysis resistance with subthreshold operation through simulations.

1.2 Previous Work

Since the early years of CMOS technology, it has been well known that the power consumption is reduced when lowering the supply voltage. A CMOS counter circuit using reduced supply voltage was presented by Leuenberger and Vittoz in 1969 [10]. The effect of voltage scaling for reducing the power consumption of a CMOS counter circuit was explored. Operating transistors in the subthreshold region has been a well known method for reducing the power consumption for a long time. In 1972, Swanson and Meindl explored the lower bounds of supply voltage [11], which they derived as $8kT/q$, approximately 200 mV at room temperature. This limit has later been reduced.

Subthreshold operation has gained renewed research interest in recent years as the demand for low power devices has increased. Research activity on the subthreshold operation increased in the early 90's. E.g. Burr and Shott reported an encoder/decoder circuit in 1994 operating at 200 mV [12].

In this millennium there has been a lot of research on subthreshold operation, e.g. at Massachusetts Institute of Technology, Purdue University and University of California, Berkeley. Some subthreshold circuit implementations are listed in Tab. 1.1. Works in the area of minimizing energy consumption [13, 14, 15], optimizing devices' performance [16] and increasing the robustness of subthreshold logic [17] are also worth mentioning. After this work was initiated the only extensive work known on sequencing elements in subthreshold operation is a comparative study on flip-flops by Fu

Table 1.1: Overview of some subthreshold applications

Year	Application	Ref
1994	Encoder-decoder circuit at 200 mV	[12]
2005	FFT-processor at 180 mV	[15]
2006	SRAM circuit at 190 mV	[19]
2007	Add-Compare-Select (ACS) unit at 180 mV	[20]
2007	SRAM circuit at 160 mV	[21]
2007	Programmable Register file at 200 mV	[22]
2008	CPU processor below 200 mV	[23]

and Ampadu published in 2007 [18].

Side-channel attacks on electronic circuit was first reported by Kocher *et al.* in 1996 [24]. Three years later Kocher *et al.* introduced power analysis attacks [5]. After the theoretical introduction to these attacks by Kocher *et al.* the topic has gained much interest in recent years. Practical implementations of attacks have been presented, as well as means of improving resistance against attacks.

1.3 Overview of the Thesis

This thesis examines subthreshold operation for reducing power consumption and protection against power analysis attacks of digital CMOS circuits.

The thesis includes a collection of 3 published papers and one unpublished paper, which will be submitted for conference inclusion.

- Paper I presents seven subthreshold flip-flop cells characterized with respect to metrics such as speed, power dissipation, Power Delay Product and Energy-Delay Product.
- Paper II takes a deeper look at three flip-flop cells, which are characterized both in a 65 nm and 90 nm process. Differences between technologies are presented and simulations in different process corners are performed.
- Paper III examines the effect of subthreshold operation for increasing resistance against power analysis attacks by simulations on an 8-bit full-adder circuit.
- Paper IV contains further examinations on the effect of subthreshold operation for increased resistance against power analysis attacks on the implementation of the AES S-box.

In addition to the technical papers, a separate introduction to the work (this part) is organized as followed:

- Chapter 1 presents the motivation for working with digital subthreshold CMOS and lists a selection of previous works done on topics of interest.
- Chapter 2 gives an introduction to subthreshold CMOS modelling and power estimation.
- Chapter 3 presents the operation of flip-flops and different measures for comparing the performance of different flip-flops.
- Chapter 4 gives an introduction to side channel attacks and reported countermeasures against them.
- Chapter 5 gives a brief introduction to the Advanced Encryption Standard and presents the implementation of the Rijndael S-Box.
- Chapter 6 presents a summarization of the included papers.
- Chapter 7 is a discussion of this thesis contributions.
- Chapter 8 gives a summarization and conclusion to the work done in this thesis, and lists some ideas for future work in the field discussed.

Two appendices are also included:

- Appendix A includes schematic drawings and transistor sizing of CMOS cells used in this thesis and included papers.
- Appendix B presents additional simulation results (not published).

Chapter 2

Subthreshold Operation

2.1 Introduction

Among the most promising methods for reducing the power consumption of VLSI, reducing the power supply voltage offers the most direct and dramatic means of reducing the power consumption [25, 9]. Presently, subthreshold operation is considered to be the most energy-efficient solution for low-power applications where performance is of secondary importance [15, 26].

A transistor is said to operate in its subthreshold region when the gate-source voltage, V_{gs}, is below the absolute voltage of the transistor's threshold voltage, V_t. The power supply voltage, V_{DD}, is reduced below the threshold voltage for ensuring subthreshold operation.

As the technology evolution proceeds, mobile electronic devices are continuously emerging in new areas with new usability. This leads to an increasing demand for device designs offering low power consumption. Reducing the power consumption with subthreshold operation has been known for decades [11]. In recent years, subthreshold operation has received more attention due to the increasing demand for power-efficient electronics. Applications well suitable for subthreshold operations include wearable medical equipment such as hearing aids and pacemakers, wrist-watch computers, self-powered devices and wireless sensor networks [27, 15, 28].

2.2 CMOS Power Consumption

CMOS has emerged as the mainstream technology in modern VLSI design during the past decades. A major factor contributing to the success of CMOS over the past decades has been its power consumption characteristic. In traditional CMOS technologies operating with a power supply voltage well above the transistor's threshold voltage, V_t, significant

power consumption only occurs during transistor switching between on and off state.

When estimating the total power consumption in a device or system two different power dissipation components must be taken into account. *Dynamic power consumption* is due to charging and discharging of load capacitance and short-circuit current drawn directly from the power supply to ground when both pMOS and nMOS transistors are partially on. *Static power consumption* is always present in a powered up circuit. This component is due to non-ideal currents of CMOS transistors.

The total power consumption can be expressed as the sum of these two components [29]:

$$P_{\text{total}} = P_{\text{static}} + P_{\text{dynamic}} \tag{2.1}$$

Static power consumption has traditionally been a negligible part of the total power consumption compared to the dynamic power consumption. But due to increased leakage it must be taken into account in modern CMOS processes. The understanding of the static power consumption is therefore important for estimating power consumption in modern CMOS technologies. The static power consumption is a composition of different leakage currents. Static power dissipation is mainly due to *subthreshold leakage current* and *gate leakage current* [29]. Other leakage effects include junction leakage, hot-carrier injection leakage, gate-induced drain leakage (GIDL) and punch-through leakage currents [30].

2.2.1 Traditional Modelling of Power Consumption

The dynamic component of the power consumption has been dominating in traditional CMOS technologies, and static power consumption has usually not been taken into account when estimating the total power consumption. Taking only the dynamic power consumption into account, power dissipation occurs only when a transistor changes state by charging and discharging the load capacitance. The current drawn from the power supply during these transitions is illustrated in Fig. 2.1. In a digital integrated circuit system such capacitances are mainly input gates of the next transistors in the signal path.

The average dynamic power consumption is a square function of the supply voltage V_{DD}, and can be approximated to [31]:

$$P_{\text{dynamic}} = \frac{1}{2} \cdot \alpha \cdot C_{\text{L}} \cdot V_{\text{DD}}^2 \cdot f \tag{2.2}$$

where α is the probability of a signal transition within a clock period ($0 \leq \alpha \leq 1$), C_{L} is the circuit capacitance to switch, V_{DD} is the power supply voltage and f is the clock frequency.

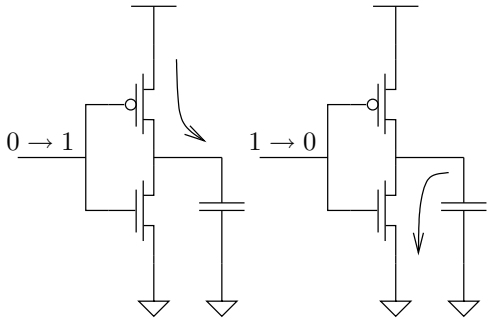


Figure 2.1: Current flows in a CMOS inverter during transitions

2.2.2 Leakage Current Problems in Modern CMOS System

The instantaneous power, $P(t)$, drawn from the power supply is proportional to the supply current, $i_{\mathrm{DD}}(t)$, and the supply voltage, V_{DD}. Over the past decades V_{DD} has decreased from typical 5 V down to typical 1 V in present state-of-the-art processes. As the dynamic power consumption quadratically depends on the supply voltage, according to Eq. 2.2, a result of this has been a dramatic reduction in the dynamic power consumption. While the dynamic power consumption has decreased, the static leakage currents have simultaneous increased, due to thinner gate-channel isolation layer and lowered threshold voltage.

Subthreshold leakage current is the current flowing between the source and drain node of a Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET) when the gate-to-source voltage, V_{gs}, is below the threshold voltage, V_t.

As the leakage current increases exponential when threshold voltage decreases, leakage is emerging as a major problem for modern deep submicron CMOS processes. Subthreshold leakage power can consume as much as 60 % of the total power in a 65 nm technology [32]. A formula for modelling the subthreshold leakage current is given in Sec. 2.3.

Although subthreshold leakage is considered an undesirable effect by most digital circuits, it is the cornerstone in subthreshold circuits. Subthreshold circuits utilize the leakage current as the conduction current.

The gate leakage current is the current flowing through the oxide layer insulating the gate from the channel. Thickness of the oxide layer has decreased proportional to V_{DD} [33]. The probability of carriers tunneling through the insulating layer increases exponentially with decreased oxide thickness. For gate oxide thickness less than 15-20 Å, gate leakage current becomes comparable to subthreshold current [29]. The gate leakage current contribution was simulated to 40 % of the total inverter off current in a 90 nm process in [13]. The contribution to the total leakage current is

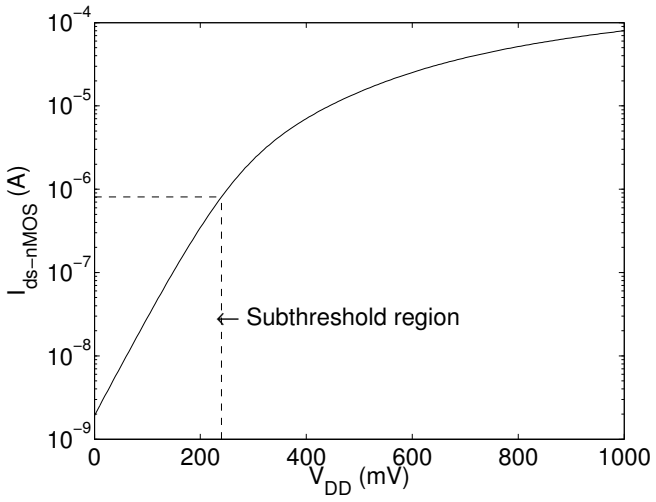


Figure 2.2: nMOS transistor current I_{ds} as a function of V_{DD}, $V_{\mathrm{gs}} = V_{\mathrm{DD}}$

rapidly diminished when the supply voltage is decreased.

The on-current going through a N-channel MOSFET (nMOS)-transistor, I_{ds}, in a 90 nm CMOS process is plotted as the function of the power supply voltage, V_{DD}, in Fig. 2.2. As seen in the figure, the $I_{\mathrm{on}}/I_{\mathrm{off}}$ ratio can be reduced with as much as a factor of approximately 10^3 if V_{DD} is reduced from 1 V down to 150 mV.

By operating the circuit's transistors in their subthreshold region, transistors are never fully turned on. Instead they are varying between being turned off and partially turned on, starting to conduct subthreshold leakage current to a greater degree. While the dynamic power consumption increases quadratically with the supply voltage, the maximum clock frequency increases only linearly with the supply voltage [4]. The static power consumption contribution exceeds the dynamic when operating at very low supply voltage [13].

When transistors are operated in the subthreshold region, power consumption is dramatically reduced without the need for major design changes of the circuit. This region has been regarded as the 'OFF' region in traditional circuit design.

2.3 Modelling of Subthreshold Leakage Current

It is essential to use an accurate model for calculating the subthreshold leakage current and other currents present in this region for estimation of power consumption. A list of important parameters influencing a transistor's subthreshold drain-source current is given in Tab. 2.1.

The drain current of a nMOS transistor operating in subthreshold,

Table 2.1: Important MOSFET subthreshold current model parameters

Symbol	Description	Unit
$v_T = \frac{kT}{q}$	Thermodynamic Voltage	V
V_t	Threshold voltage	V
V_0	Early voltage	V
n	Slope factor	no unit
μ	Mobility of electrons in the channel	$m^2/(V \cdot s)$
C_{ox}	Oxide capacitance per unit area	F/m^2
$\frac{W}{L}$	Width/length ratio	no unit
κ	Technology dependent constant	no unit

$V_{\mathrm{gs}} < V_t$, can be modelled as [26]:

$$I_{\mathrm{ds}} = I_0 e^{\frac{\kappa V_{\mathrm{gs}}}{v_T}} e^{(1-\kappa)\frac{V_{\mathrm{bs}}}{v_T}} \left(1 - e^{\frac{-V_{\mathrm{ds}}}{v_T}} + \frac{V_{\mathrm{ds}}}{V_0}\right) \tag{2.3}$$

where I_0 is the zero-bias current for the device, as given in Eq. 2.4. V_{gs} is the gate-to-source potential, V_{ds} is the drain-to-source potential and V_{bs} is the substrate-to-source potential (body-bias). V_0 is the Early voltage, proportional to the channel length. κ gives the effectiveness for which the gate potential is controlling the channel current, normally in the range 0.7-0.75 [26]. The thermal voltage, v_T, is calculated as $v_T = kT/q$, where k is the Boltzmann's constant, T is the temperature and q is the elementary charge. At room temperature (T = 300 K), v_T is about 26 mV. The threshold voltage, V_t, varies with length, width, V_{ds}, V_{bs}, temperature and processing [29], as well as the body effect as described in Sec. 2.6.

Typical parameters for a 2 μm n-well process are $I_0 = 0.72$ aA, $\kappa = 0.75$ and $V_0 = 15$ V [26]. The current changes by a factor 10 for an 80 mV change in V_{gs} or a 240 mV change in V_{bs} (up to 100 nA, which is the limit of the subthreshold region).

I_0 may be expressed as [34]:

$$I_0 = 2n\beta v_T^2 = 2n\mu_n C_{ox} \frac{W}{L} v_T^2 \tag{2.4}$$

where β is the technology dependent transconductance factor.

2.4 Lower Bounds of CMOS Supply Voltage

Swanson and Meindl derived in 1972 equations suggesting a minimum useful supply voltage of $8kT/q$ for inverters operating in weak inversion

Table 2.2: Ideal-case minimum supply voltage V_{DD} for given circuit design constraints [4]

Constraint		V_{DDmin} ($T = 300\,\mathrm{K}$)	V_{DDmin} [v_T]
$A_{max} > 1$	(ring oscillator)	36 mV	1.40
$NM > 10\%$	(inverter)	55 mV	2.13
$A_{max} > 4$	(standard design)	83 mV	3.22
$F_U > 9$	(fan-in of 3)	83 mV	3.22
$I_{on}/I_{off} > 10^4$	(dynamic logic)	238 mV	9.22

[11]. At room temperature this compares to approximately 200 mV. By further research in the area, Schrom *et al.* reported in 1996 an analytic absolute lower bound of supply voltage [4]. This absolute lower bound assumes ideal and perfectly symmetrical devices, not likely achievable by any CMOS technology according to [35]. The lowest bounds of supply voltage for a CMOS inverter is 36 mV at a temperature of 300 K, corresponding to the *minimum-inverter-gain criterion*.

Achievable values for minimum supply voltage for various design constraints, calculated and presented in [4], are listed in Tab. 2.2. Minimum supply voltage V_{DD} is given in millivolts on a temperature of 300 K, and may be estimated for other temperatures by a factor of $n = S/(v_T \ln(10))$ where S is an achievable average gate swing as a worst-case estimate for subthreshold operation [4].

A minimum of logic function, such as NAND, NOR and XOR, is required to operate successfully in most circuit implementations for practical use. In practical use a minimum value of V_{DD} may be around 83 mV, according to Tab. 2.2.

2.5 Sizing for Subthreshold Operation

For optimal performance, transistors in a pull-up and pull-down network should be able to drive the same current. In traditional design, pMOS sizing is done proportionally to nMOS with the relationship $W_{\mathrm{p}} = 2 \cdot W_{\mathrm{n}}$. But the optimum pMOS/nMOS ratio varies with the supply voltage. In the subthreshold region it is highly dependent on process variation as well [15]. Requirements for power consumption, minimum supply voltage and yield requirements must be taken into accounts when dimensioning transistors.

Minimum sized devices minimize power consumption but can reduce the functionality of circuits at low supply voltages, thus limiting the minimum supply voltage [36]. Minimum sized devices are theoretically

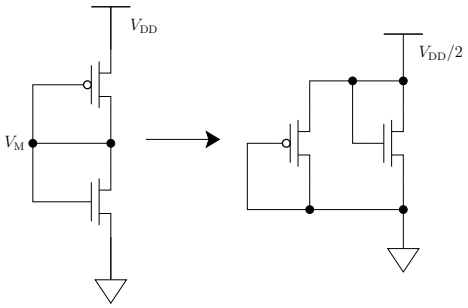
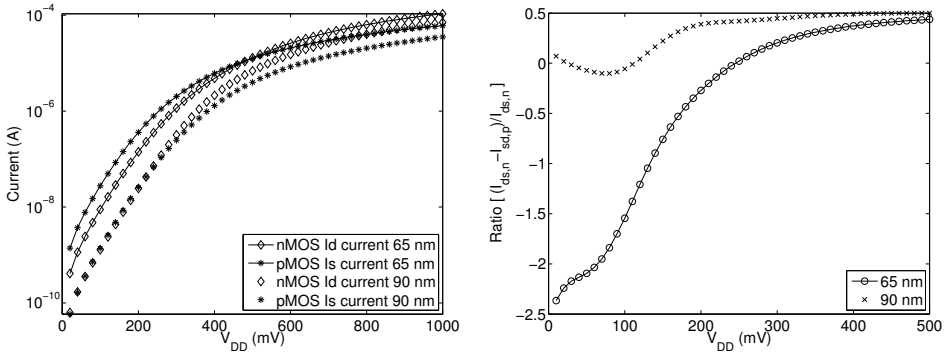


Figure 2.3: Small-signal equivalent of inverter for width optimization



(a) Transistor current I_{ds} as a function of V_{DD}

(b) Ratio between nMOS and pMOS currents in 65 nm and 90 nm process with $W_n = W_p$ and $L_n = L_p$

Figure 2.4: Transistor channel conduction at different supply voltages

optimal for reducing energy per operation when accounting for the impact of sizing on voltage and energy consumed [13].

Symmetrical devices give minimum V_{DD} operation [36]. The optimum pMOS/nMOS width ratio for minimum V_{DD} can be obtained by comparing currents in the devices. With the setup from Fig. 2.3, the transistor current as a function of V_{DD} is plotted in Fig. 2.4(a), with $V_{gs} = V_{DD}$ for the STMicroelectronics 90 nm and 65 nm general purpose processes. The corresponding n/p ratios are calculated and plotted in Fig. 2.4(b). For both plots minimum sized transistors with $W_n = W_p$ and $L_n = L_p$ have been used. Remembering that the current through the transistor is linear dependent on the W/N the ideal W_p/W_n ratio can be found.

The variation in threshold voltage due to random doping fluctuations is proportional to $1/\sqrt{WL}$, causing minimum sized devices to produce the worst case random V_t variations [14].

2.6 Body-Bias Regulation

The body effect is a second-order effect, occurring due to potential difference between the source and body of a transistor [29]. It can be modelled as an increase in the threshold voltage V_t for a nMOS transistor that occurs when the source and substrate have different voltage potentials. With this effect taken into account, the threshold voltage for a n-channel transistor is[37]:

$$V_\mathrm{t} = V_{\mathrm{t}0} + \gamma \left(\sqrt{V_\mathrm{sb} + |2\Phi_\mathrm{F}|} - \sqrt{|2\Phi_\mathrm{F}|} \right) \tag{2.5}$$

where $V_{\mathrm{t}0}$ is the threshold voltage without body effect ($V_\mathrm{sb} = 0$), Φ_F is the difference between the Fermi potential of the substrate and intrinsic silicon (approximated to 0.35 V at room temperature for typical doping levels). The factor γ, often called the *body-effect constant*, is:

$$\gamma = \frac{\sqrt{2qN_\mathrm{A}K_\mathrm{S}\varepsilon_0}}{C_\mathrm{ox}} \tag{2.6}$$

where N_A is the doping concentration, K_S is the relative permittivity of silicon, ε_0 is the permittivity of free space and C_ox is the gate oxide capacitance. The body-effect constant is proportional to the doping concentration.

Body-bias regulation can improve the inverse subthreshold slope S due to reduced short-channel effects and reduce the junction capacitances by increasing the junction depletion widths [16]. These effects lead to faster operation and lower power consumption in a subthreshold device. For example, a 19% decrase in the switching delay and 30% reduction in the Power-Delay Product (PDP) of an inverter is obtained in [16] by applying a reverse body-bias of 150 mV.

Body-bias regulation has been presented as a promising method for decreasing V_t variations [38]. Threshold voltage is stabilized by regulating the back-gate voltage of transistor with a small bias regulator circuit.

Chapter 3

Sequential Computing

A major part of digital VLSI systems is designed as a *clocked sequential system*, using a global clock to synchronize the system. The activity of such a system is controlled by the global clock, which triggers registers all over the system at the same time.

A *sequencing element*, connected to the global clock, is used to synchronize data. Combinational logic is placed between the sequencing elements, as illustrated in Fig. 3.1. The purpose of a sequencing element is to enforce sequence, to distinguish the current token from the previous or next token [29].

The two most commonly used sequencing elements are *flip-flops* and *latches*. Flip-flops and latches can mainly be separated into how the output signal is changed when the input signal changes. When the input signal flows directly through to the output the element is said to be *transparent*. Latches are transparent while the clock signal is high, while flip-flops are not transparent at any time.

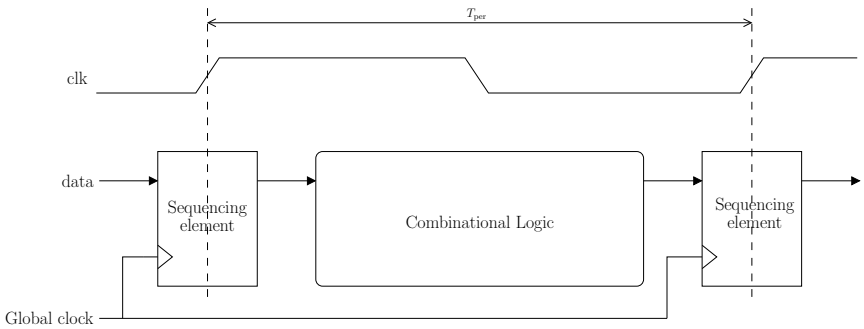


Figure 3.1: Clocked sequential system

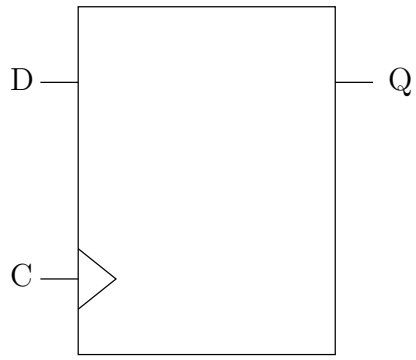


Figure 3.2: D flip-flop symbol

3.1 Flip-Flops

Flip-flops are an important building block in modern digital VLSI systems. Some of the major usage areas of flip-flops are in registers, pipelines and state machines, ensuring sequencing of data.

A flip-flop has the ability to read an input value, save it for some time and then write the stored value somewhere else, even if the element's input value has subsequently changed.

Based on the comparison of the power breakdown for different elements in VLSI chips, latches and flip-flops are the major source of the power consumption in synchronous systems [39]. Flip-flops have a direct impact on power consumption and speed of VLSI systems. Therefore study on low-power performance of flip-flops are important. When estimating the power dissipation of a system, flip-flops may be a major power consumption component.

In this thesis, the *delay flip-flop* (D flip-flop) is used [40]. This type of flip-flops can be interpreted as a primitive delay line or zero-order hold, since the data is posted at the output one clock cycle after it arrives at the input. It is called delay flip-flop because the output takes the value of data-in from the previous clock period.

The operation of a D flip-flop can be expressed as:

$$Q_{\text{next}} = D \tag{3.1}$$

where Q_{next} is the output value in the next clock period and D is the input value sampled at the rising edge of the clock signal for the start of the clock period.

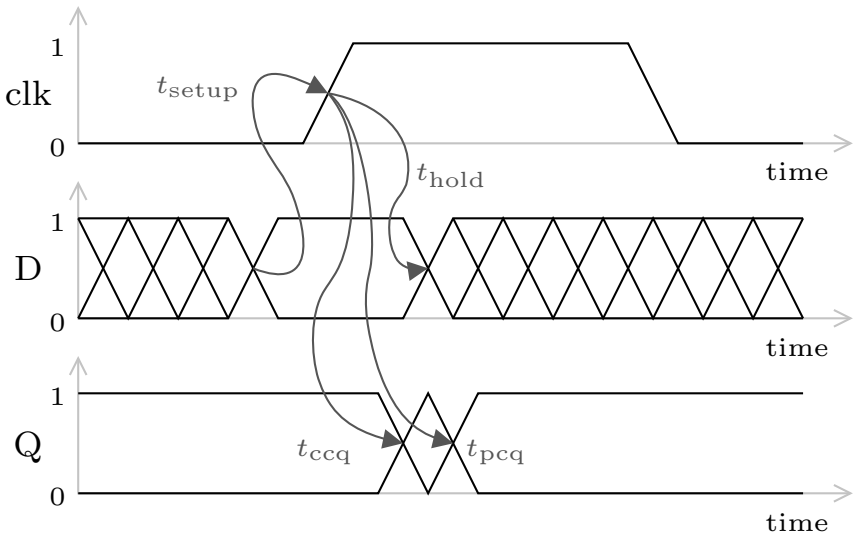


Figure 3.3: Flip-flop timing diagram

3.2 Flip-Flop Performance Characterization

Significant parameters in characterizing a flip-flop's performance are its delay time and power dissipation. An optimal flip-flop design has low power consumption, imposes no delay and gives a valid output at all time. Trade-offs between these parameters must be done in practical implementation.

3.2.1 Timing and Delay

For estimating the performance of a flip-flop, three important timings and delays are used: (1) propagation delay, (2) setup time and (3) hold time. Setup and hold time define the relationship between the clock and input data, while the propagation delay defines the relationship between the internal delay for the input signal to propagate through the flip-flop and change the output signal.

The total delay of a sequencing element can be expressed as the time from the input signal changes its state to the output signal is stabilized.

A flip-flop can capture an input signal even though it arrives later than the setup time, but the propagation delay might increase, resulting in a large total delay[29].

Propagation Delay

The propagation delay of a flip-flop is defined as its clock-to-output delay. This equals the maximum delay from the arrival of the clock's active edge

to the output of the flip-flop is considered stable. Usually the propagation delay differs from low to high transition and high to low transition. By definition, the delay is the maximum value of these two delay:

$$t_{pcq} = \max\left(t_{pcq_{LH}}, t_{pcq_{HL}}\right) \tag{3.2}$$

Clock Contamination Delay

The clock contamination delay is the minimum time from the clock changes to the output is available that occurs when the data input arrives early. I.e. the time it takes from the clock goes high to a valid output signal is available.

$$t_{ccq} = \max\left(t_{ccq_{LH}}, t_{ccq_{HL}}\right) \tag{3.3}$$

Setup Time

The input must be stable for some time before the flip-flop triggers at the clock edge. The setup time is defined as the time the data value must remain stable around the arrival of the clock's active edge to ensure that the flip-flop retains the proper output value.

The setup time may differ for a low-to-high and high-to-low transition. Setup time is by definition the maximum of these values:

$$t_{\text{setup}} = \max\left(t_{\text{setup,LH}}, t_{\text{setup,HL}}\right) \tag{3.4}$$

Hold Time

After the clock signal has changed, the input must be hold for a period of time to allow the signal to propagate through the flip-flop for ensuring a stable output. This delay time is called *hold time*. The hold time may be negative, which means that the input signal may change before the clock changes and still ensuring the proper output value. As for other timing measurements, the hold time may differ for a low-to-high and high-to-low transition. The hold time is defined as:

$$t_{\text{hold}} = \max\left(t_{\text{hold,LH}}, t_{\text{hold,HL}}\right) \tag{3.5}$$

Total Delay

The delay of a flip-flop can be expressed as the time taken from the input changes its state to the output has stabilized. The total delay can be expressed as $t_{\text{delay}} = t_{\text{setup}} + t_{\text{pcq}}$, where t_{setup} is the time taken for the input to propagate and stabilize in the flip-flop, and t_{pcq} is the time taken from the clock goes high to a valid output Q is available.

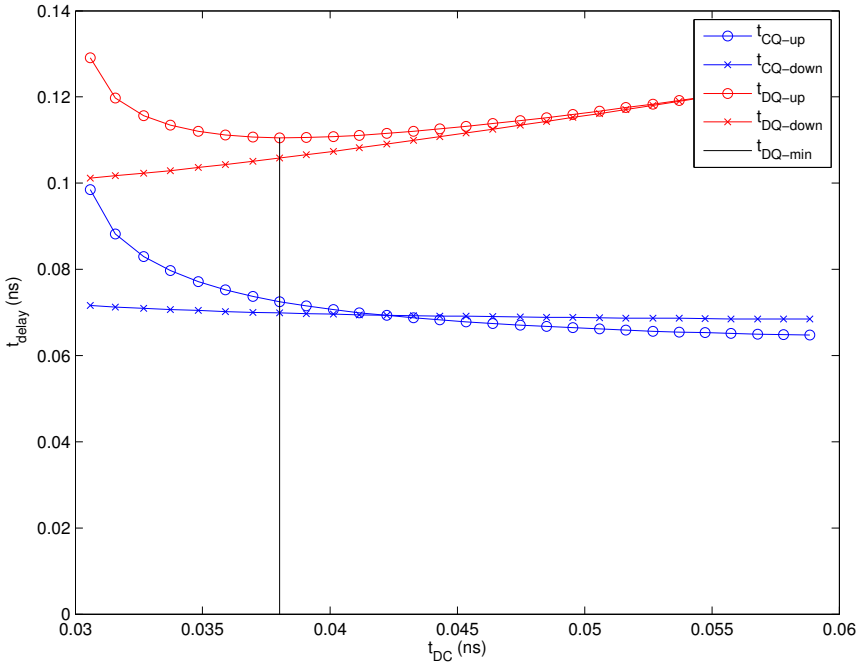


Figure 3.4: PowerPC 603 flip-flop: t_{delay} vs t_{setup}

In Fig. 3.4 simulation of t_{delay} vs. t_{setup} has been done at $V_{\text{DD}} = 200\,\text{mV}$. It is clearly shown how the delay is directly dependent on the time the input signal arrives in relationship to the clock signal. At the left side of the plot, the input signal exceeds the clock edge, and the output is not valid. At the right side the output signal monolithically grows due to increased t_{setup}.

3.2.2 Power Consumption

A common method for measuring the power consumption of a flip-flop is to operate the flip-flop at maximum operating frequency with a maximum power consumption pattern applied on the input. The power consumption is then measured as the average supply current drawn by the flip-flop with input buffers and some load taken into account.

The average power consumption P can be defined:

$$P = i_{V_{\text{DD}}avg} \cdot V_{\text{DD}} \tag{3.6}$$

where $i_{V_{\text{DD}}avg}$ is the average current drawn from the power supply by the circuit over the time being measured and V_{DD} is the power supply voltage.

3.2.3 Performance Metrics

Power-Delay Product

Both power and delay are metrics which can be adjusted individually. Therefore they are usually not considered as good figure-of-merits for a design or circuit. The Power-Delay Product (PDP) is the product of delay time and power consumption, taking both metrics into account. PDP is considered a good figure of merit for a circuit's performance.

PDP is calculated as:

$$PDP = t_{\text{delay}} \cdot P \tag{3.7}$$

where t_{delay} is the delay found in Sec. 3.2.1 and P is the power consumption, as defined in Sec. 3.2.2.

Energy-Delay Product

The Energy-Delay Product (EDP) weights the execution time more than PDP. EDP is considered a relatively implementation neutral metric, causing architectural improvements contributing most to both performance and energy efficiency to stand out [41].

EDP can be expressed as:

$$EDP = PDP \cdot t_{\text{delay}} = t_{\text{delay}} \cdot t_{\text{delay}} \cdot P \tag{3.8}$$

where PDP is the Power-Delay Product found in Sec. 3.2.3, t_{delay} is the delay found in Sec. 3.2.1 and P is the power consumption, as defined in Sec. 3.2.2.

3.2.4 Metastability

A flip-flop is a *bistable device*, meaning it has two stable states (0 and 1).

The binary decision which the flip-flop must take to set the output can take an unbounded amount of time in the case of colliding inputs [42]. When a flip-flop experience this, it is said to be in a *metastable state* where the output is at an indeterminate level between 0 and 1 [29].

When the output of a flip-flop in a metastable state is sampled by other digital circuitry, non-binary signals will propagate through the binary systems. This effect is called a *synchronization failure*.

Metastable states cannot be totally avoided when designing a systems, but the probability of occurrence can be made reasonably small with careful consideration of timing.

3.3 Flip-Flop Designs

The basic method for designing a flip-flop cell is to combine two latches with complementary non-overlapping clock signals. Two common types of characterization of flip-flop designs is to separate them into *static* and *dynamic* designs.

Static flip-flop designs have some sort of feedback to retain its output value indefinitely. Dynamic flip-flop designs do not have this type of feedback, generally maintaining their value as charge on capacitors. If the flip-flop is not refreshed for a long period of time, the charge will leak away [29]. A static master-slave flip-flop cell can be made dynamic by removing its feed-back elements. Dynamic flip-flops are prone to internal dynamic node discharge. The storage capacitances in a dynamic flip-flop must be periodically refreshed, otherwise the charge on these nodes will leak away resulting in invalid data [39].

Another commonly used flip-flop design is sense-amplified based flip-flops. A sense-amplified based flip-flop has a sense amplifier on its input gates (D and its complementary value). The sense amplifier is followed by a normal static latch to retain the output signal.

Many other flip-flop architectures have been presented. For example, the Semi-Dynamic Flip-Flop (SDFF) and Hybrid Latch Flip-Flop (HLFF) designs are commonly used in conventional circuit implementations. Due to their high power consumption these cells have not been considered in this thesis [39].

Schematic drawings and transistor sizings for flip-flops reviewed in Paper I and II are shown in A.2.

Chapter 4

Side-Channel Attacks

4.1 Introduction

Cryptography is extensively used in modern electronic communication for protecting message secrecy, ensuring personal privacy and proving message authenticity. Cryptographic algorithms have after extensive academic research over the past decades evolved to be secure against known mathematical cryptoanalysis attacks. However, in recent years several attacks based on the physical implementation of electronic cryptographic systems have been presented.

A cryptographic system is only as secure as its weakest link. It has become of primary concern for an increasing number of researchers that the physical implementation is the weakest link of many cryptographic systems.

This chapter intend to investigate the vulnerability against *side-channel attacks* in modern cryptographic circuits. Side-channel attacks use physical measurements of informations such as time delay, power consumption and electromagnetic radiation for finding secret keys inside the circuit.

Theoretical background on the nature of power consumption in CMOS technology, an introduction to cryptography and the different types of side-channel attacks is given in Sec. 4.2. In Sec. 4.3, proposed countermeasures against side-channel attacks are presented.

4.2 Theoretical Background

4.2.1 Cryptography

The term cryptography refers to the study of secret messages [43]. In modern communication over the Internet, cryptography is of primary importance for secure communication, keeping privacy, ensuring message authenticity and access control. Information transmitted over the Internet

passes nodes neither controlled by the sender nor the receiver and may easily be eavesdropped.

The purpose of an encryption algorithm is to protect the secrecy of messages sent over an insecure channel [44].

Lots of processing are required for encryption and decryption of data. With large data flows, dedicated cryptographic hardware is used to keep up with the speed. Dedicated cryptographic hardware is also considered to be more secure than software implementation because secret cryptographic keys can be kept in a controlled environment, specially designed for secure keeping. Nevertheless, cryptographic ICs are also vulnerable against break-in-attempts. Attempts on breaking in through the physical implementation of a cryptographic IC are called *side-channel attacks*.

A *cipher* is a cryptographic algorithm for transposing a known input text to be hidden from eavesdropping, *plaintext*, into a ciphertext. A *ciphertext* contains the same information as the plaintext, but in a format not readable unless you know the cipher being used and a secret *key*. The key is used as an input to the cipher and controls the operation of the cipher. Without a correct key it is impossible to transform the ciphertext back into the original plaintext.

Encryption, or enciphering, is the transformation of a plaintext P into a ciphertext C. The operation is performed by a cipher as $C = E_K(P)$, where E is the encryption algorithm of the cipher and K is the provided key.

Decryption, or deciphering, of a ciphertext C is the transformation back to readable text by the receiver, by performing $P = D_K(C) = D_K(E_K(P))$, where D is the decryption algorithm.

Ciphers can be divided into two main categories, transposition and substitution ciphers. *Substitution ciphers* replace letters or large blocks with substitutes. *Transposition ciphers* rearrange the letters in the plaintext.

Product ciphers are created by composing substitution and transposition ciphers. The cryptographic ciphers defined by the US National Institute of Standard and Technology (NIST) as the Data Encryption Standard (DES) [43] in 1976, as well as its proceeder, the Rijndael cipher [43], selected as the Advanced Encryption Standard (AES) by NIST in 2002, are well known examples of product ciphers used as a base in major communication systems today.

4.2.2 Side-Channel Attacks

Modern ciphers are designed to be immune against known cryptoanalysis methods, and therefore attacks on them are hard to perform. But when cryptography is used in computer systems these ciphers are prone to attack on the physical implementation.

A cipher implemented in an electronic circuit produces timing information, power consumptions variations due to switching activity and radi-

ates electromagnetic energy, which can easily be measured at low costs [5]. Such side channel informations can provide a source of information which can be used to break the cryptographic circuit in order to recover the secret encryption key the device is using.

Side-channel attacks can be categorized by the side-channel information they are exploiting. The first theoretical presentation of a side-channel attack was reported by Kocher in 1996 [24], analyzing the difference in time used by different inputs.

Kocher presented the concept of power analysis attack in 1999 [5]. This type of attack was performed on an actual implementation of a cryptographic circuit by Örs in 2004 [45]. Power analysis attack uses the variation in power consumption correlated to the operations done in calculating the secret key being used.

A side-channel attack may require considerable technical knowledge of the internal operation of the system on which the cryptographic algorithm is implemented.

Timing Attack

Implementations of cryptographic systems where the execution time of certain operations differs depending on the input values are vulnerable against *timing attacks*. Differences in the execution time are often deliberately implemented in the algorithm by the designer for performance optimization. Kocher showed in [24] that it is possible to find the entire secret key of a vulnerable cryptographic system only by timing measurements.

By careful algorithmic and electronic design, timing attacks can be completely avoided by making the system run in fixed time.

Simple Power Analysis Attack

In a *simple power analysis (SPA)* attack, the power consumption of a cryptographic IC is measured directly during cryptographic operations. Using a set of power consumption measurements taken across a cryptographic operation an attacker can directly determine information about a device's operation and the secret key [5].

SPA can be used to break cryptographic implementations in which the execution path depends on the data being processed, exploiting the relationship between the executed operations and the power leakage [45].

Differential Power Analysis Attack

While SPA attacks are used to reveal power variations in the execution path due to the instruction sequence, *differential power analysis (DPA)* attacks can

reveal effects correlated to data values being manipulated [5]. This type of attack is also referred to as *correlation power analysis* [46].

A differential power analysis attack is hard to protect against, as it uses statistical and error-correcting methods to extract secret information from a power consumption signal [47].

In a DPA attack, the attacker uses a prediction model of the device being attacked. This model is used for predicting the amount of side-channel output for a certain moment of time in the execution of the cipher. These predictions are correlated to the real side-channel output of the circuit by applying statistical methods. Some common statistical methods used in DPA are the *distance-of-mean* test and the *correlation analysis* [45].

Electromagnetic Radiation Attack

Electromagnetic radiation is leaked from all electronic devices. A magnetic field is produced when motion occurs in the electronic current flowing in the circuits. An *electromagnetic analysis* (EMA) attack measures the electromagnetic radiation, and the attack can be performed during the same methods as for power attacks [48].

Fault Analysis Attack

Fault analysis attacks are not directly side-channel attacks. They can be placed under the category of implementation attacks, as they exploit the physical working environment required by the system.

Fault analysis attacks can be divided into two categories. A *differential fault analysis* attack exploits a circuit by changing the operating voltage, tampering with the clock, or applying radiation of various types to the circuit. By measuring the output differences from the output of the circuit at normal operation, a circuit vulnerable to differential fault analysis attacks may reveal secret key information.

A *non-differential fault analysis* attack is based on causing permanent damage to a circuit for the purpose of extracting symmetric keys.

4.3 Countermeasures against Side-Channel Attacks

The goal of countermeasures against side-channel attacks are to decrease or preferably completely remove any side channel information leaked by the chip.

Countermeasures can be done at several layers of the cryptographic system. Beginning on the top-level, protocol and algorithmic countermeasures can be done. At a lower lever, physical electronic countermeasures can reduce the side channel information emitted. Fig. 4.1 illustrates the

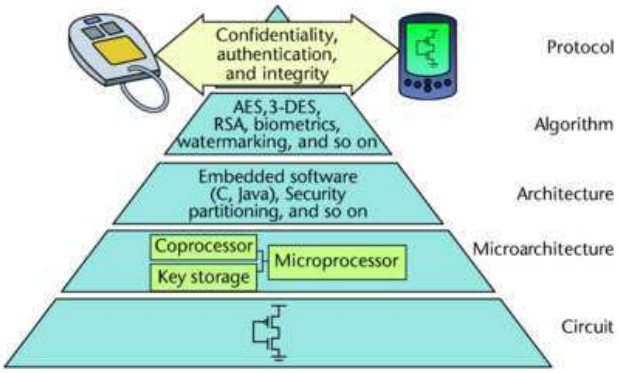


Figure 4.1: Security pyramid of an embedded system [49]

different layers. To ensure security in embedded systems, security measures must be addressed in all abstraction layers [49].

4.3.1 Algorithmic Countermeasures

Algorithmic countermeasures address the problem of side-channel attacks in the design of a cryptographic algorithm. By taking realistic assumptions about the underlying hardware into account when designing a cryptographic system, side-channel attacks can be made much more difficult to accomplish.

For example, nonlinear key update procedures can be employed to ensure that power traces cannot be correlated between transactions [50]. Aggressive use of exponent and modulus modification processes in public key schemes can also be used to prevent attackers from accumulating data across large numbers of operation [50].

This may solve the problem, but it does require design changes in the algorithms and protocols themselves, which are likely to make the resulting product non-compliant with standards and specifications.

4.3.2 Electronic Countermeasures

Electronic countermeasures are taken on the hardware design level. The goal of such countermeasures is to minimize side-channel information leakage by careful design of the logic gates. Such countermeasures are independent of the cryptography algorithm and may be implemented as standard hardware libraries [8].

Blinding

Kocher proposed in [24] a technique for preventing timing attack. By adapting techniques used for blinding digital signatures it is possible to prevent the attacker from knowing the input of the modular exponentiation operation. The correlation between the input data known to the attacker and the time used is removed. This makes it impossible to calculate the secret key by timing attacks, while the cipher still may use performance optimization on modular exponentiation operations.

Adding noise

Adding noise to a signal helps hiding the secret key, because the statistical evaluation is worse and it is required more measurements if it is noisy. It is important to ensure that added noise does not affects the internal operations of the chip, as it may cause malfunction.

Reducing signal variation

The ultimate goal of a reduction in the signal variation is to attain a constant power consumption. In [8], Tiri specifies two conditions which must be satisfied to have a constant power consumption:

- a logic gate must have exactly one switching event per signal transition
- the logic gate must charge a constant capacitance in that switching event

Some differential logic styles have been presented to meet these conditions. For instance, *wave dynamic differential logic* (WDDL) was presented in [8]. The goal of these countermeasures is to balance the power consumption of the logic gates to be insensitive to switching activity and thus not create any side-channel information.

By reducing the signal amplitude power consumption will also be decreased. An attacker will require more samples to be able to perform a differential power analysis because of more noise. However, an attacker with an infinite number of samples will still be able to perform DPA on the signal [51].

Bouesse *et al.* reduced the power supply voltage to 0.4 V [52]. The reduction in supply voltage with a factor of 3 resulted in a reduction of the energy consumption with a factor of 8.

Operating transistors in the subthreshold region reduces the signal amplitude significantly and decreases the signal-noise ratio. This will be an advantage in a cryptographic system making it harder to get side-channel information. This also has a significant effect on the power analysis.

The dynamic power consumption component is not the significant power consumption part in subthreshold region, but rather the static component, independent of the signal and switching activity.

Chapter 5

Advanced Encryption Standard Substitution Box Implementation

National Institute of Standard and Technology (NIST) announced in 1997 a competition for a new cryptographic algorithm, as the successor of the aging Data Encryption Standard (DES). In 2000, the Rijndael cipher was announced as the winner of the competition. One year later, NIST announced the new Advanced Encryption Standard (AES) algorithm as approved in Federal Information Processing Standard (FIPS) 197 [53].

The final AES algorithm is almost identical with the Rijndael algorithm, designed by Joan Daemen and Vincent Rijmen [53]. Rijndael supports a larger range of block and key sizes than AES. AES is currently one of the most popular algorithms for symmetric key ciphers [54], and is offering a straight-forward software and hardware implementation.

The best known software implementations of AES achieve about 15 cycles/byte on a modern PC [55]. Hardware implementation can speed up encryption significantly.

One of the major building block in AES is the SubBytes operation, also called Substitution box (S-box), which substitutes bits in a non-linear operation. The SubByte transformation is used to obscure the relationship between plaintext and ciphertext. In Paper IV, the S-box is implemented in 90 nm CMOS process and simulated in super- and subthreshold operation, exploring the power analysis attack resistance in subthreshold operation.

5.1 The Advanced Encryption Standard

AES is a block cipher cryptographic algorithm, operating with a block size and key length which can be chosen independently to be 128, 192

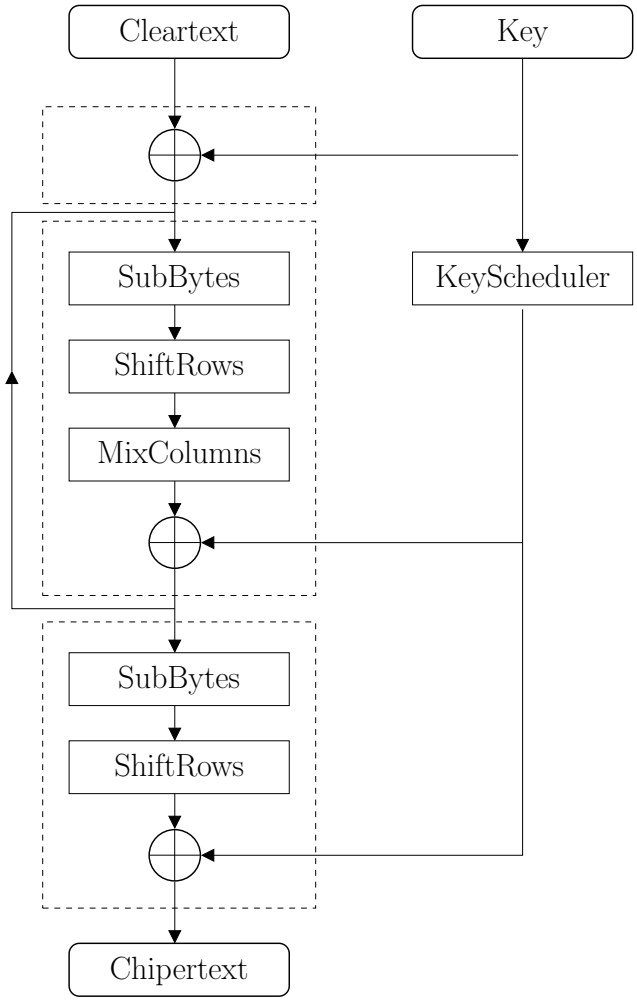


Figure 5.1: AES encryption round structure

or 256 bits. Depending on block and key lengths, a different number of steps, called *rounds*, are performed to encrypt or decrypt data. Each round consists of four operations, called *layers*: *SubBytes*, *ShiftRows*, *MixColumns* and *AddRoundKey*. According to the standard, the basic units of the AES algorithm is an 8-bit *byte*, but these operations can as well be performed on 32-bits words. The round structure of AES is illustrated in Fig. 5.1.

The *input* and *output* of the AES algorithm each consists of *sequences of 128 bits*. These sequences are referred to as blocks. The *Cipher Key* for the AES algorithm is a *sequence of 128, 192 or 256 bits*. Other input, output and Cipher Key lengths are not permitted [56].

AES is designed to be simple, resistant against all known algorithmic attacks, and to offer fast and compact code on many platforms. The major

building blocks of the AES algorithm are the non-linear S-boxes (SubByte-operation) and the MixColumn-operation. A hardware implementation may require up to 20 instances of the S-box, depending on the throughput and clock frequency requirements [57]. The implementation of the S-Boxes mainly determines the efficiency of a hardware implementation in terms of area, throughput and power consumption.

5.2 Finite Field Arithmetic

All bytes in the AES algorithm are interpreted as *finite field* elements. The following section introduces the mathematics needed for implementation of the AES S-Box.

A finite field contains a finite set of elements, completely known. Finite field arithmetic differs from standard arithmetic, as all arithmetic operations result in an element within the same field. The operations addition, subtraction, multiplication and division are defined in finite fields [58].

A field K of order p^n is denoted GF(p^n) and contains p^n elements. The letters GF are the abbreviation for *Galois field*, which is another name of finite fields, named after Évariste Galois. The prime p is the *characteristic* of the field K and the positive integer n is called the *dimension* of the field over its prime field GF(p). Each field K of order p^n must contain the prime field GF(p) [59]. When the characteristic of the field is 2, it is conventional to express elements of the field as binary numbers.

Finite fields are important in coding theory and is a central part of many cryptographic algorithms. The AES algorithm's S-box uses a finite field on the form GF(2^8).

5.2.1 Polynomial Representation of Finite Fields

It is often advantageous to represent finite fields as polynomials when doing mathematical operations. The elements of the finite field $K \in$ GF(2^n) can be represented as polynomials of degree strictly less than n with binary coefficients. The resulting polynomials are n-dimensional vectors over the binary field GF(2).

Operations are then performed modulo the *irreducible polynomial* $P(x)$ of degree n. A polynomial is irreducible if and only if its only divisors are one and itself.

For the AES algorithm, the irreducible polynomial is [56]:

$$m(x) = x^8 + x^4 + x^3 + x + 1. \tag{5.1}$$

It is possible to do operations on a reduced order field by mapping an element a from GF(2^8) to GF$(((2^2)^2)^2)$ such as the two fields are

Table 5.1: Polynomial representation of reduced fields

Field	Bit representation	Irreducible polynomial
GF(2)	b_0	n/a
GF(2^2)	$b_1\boldsymbol{x} + b_0$	$P_x(x) = x^2 + x + 1$
GF($(2^2)^2$)	$b_3\boldsymbol{xy} + b_2\boldsymbol{y} + b_1\boldsymbol{x} + b_0$	$P_y(y) = y^2 + y + \phi$ $\phi \in$ GF(2^2)
GF($((2^2)^2)^2$)	$b_7\boldsymbol{xyz} + b_6\boldsymbol{yz} + b_5\boldsymbol{xz} + b_4\boldsymbol{z}$ $+b_3\boldsymbol{xy} + b_2\boldsymbol{y} + b_1\boldsymbol{x} + b_0$	$P_z(z) = z^2 + z + \lambda$ $\lambda \in$ GF($(2^2)^2$)

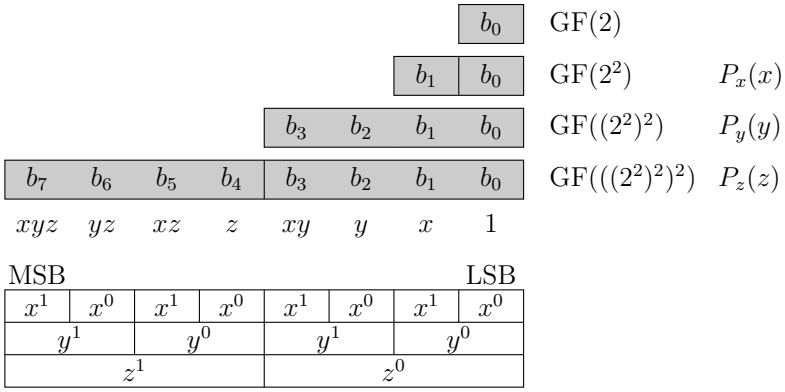


Figure 5.2: Binary representation in composite fields

isomorphic using an isomorphism. To reduce the complexity of operations elements in GF(2^{2n}) can be represented as polynomials of first degree with coefficients from GF(2^n) to reduce the complexity. The field GF(2^{2n}) is generated as an extension field of GF(2^n) using an irreducible polynomial $P(x) = x^2 + \alpha\boldsymbol{x} + \beta$, where $\alpha, \beta \in$ GF(2^n)). The field GF(2^{2n}) is then a field extension of degree 2 over GF(2^n) and can be represented as polynomials of first degree with coefficients from GF(2^n), i.e. $K = p\boldsymbol{x} + q$, $p, q \in$ GF(2^n). Any higher power of the irreducible polynomial, e.g. y^2, is reduced according to the primitive polynomial, e.g. $y^2 = y + \phi$ [60].

General polynomial representations of reduced fields in GF(2), GF(2^2), GF($(2^2)^2$) and GF($((2^2)^2)^2$) are listed in Tab. 5.1. Binary representations of polynomials in the fields are illustrated in Fig. 5.2 [60].

5.2.2 Arithmetic Operations on Finite Fields GF(2^n)

Arithmetic operations on fields with characteristic 2, i.e. GF(2^n), are of interest for the S-box implementation and will be discussed in this section. Arithmetic operations needed by the S-box are *addition*, *multiplication* and *multiplicative inverse*. Using polynomial representation, addition and multiplication are relatively trivial operations to implement in hardware.

Calculation of the multiplicative inverse of a number is not a trivial operation and will be described in the next section.

Addition is achieved by adding the coefficient for the corresponding powers in the polynomial vectors in $GF(2^n)$ for the two elements. The addition can be implemented in hardware with the binary operator exclusive OR (XOR) [58].

Multiplication in $GF(2^n)$ is defined as polynomial multiplication modulo the irreducible polynomial $P(x)$ of degree n of the field [58]. The multiplication operation can be described mathematically as:

$$\boldsymbol{p} = \boldsymbol{q} \cdot \boldsymbol{r} \bmod P(x) \tag{5.2}$$

where $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ are polynomials of order $GF(2^n)$ and $P(x)$ is the irreducible polynomial for the given field.

Unlike addition, there are no simple hardware operations that corresponds to this multiplication. The hardware implementation used for performing this operation is described in Sec. 5.4.2.

5.2.3 Multiplicative Inverse

A non-trivial and costly operation in the S-box is calculating the multiplicative inverse over the field $GF(2^8)$. The inverse of an element a, i.e. a^{-1}, is calculated such that $a \cdot a^{-1} \equiv 1 \bmod P(x)$, where $P(x)$ is the irreducible polynomial [55].

The simplest technique for finding an inverse element for any $a \in GF(2^n) \neq 0$ is using a table look-up from a pre-generated table. As the table look-up approach is costly to implement in hardware due to large area demands, it is common to use the *extended Euclidean algorithm* and composite field arithmetics to reduce the implementation size [61, 62, 55, 60].

Using the extended Euclidean algorithm, multiplicative inverse in $GF((2^n)^m)$ can be defined recursively in terms of a sub-field $GF(2^n)$ and its extension $GF((2^n)^m)$ [60]. By using polynomial representation of the finite field the problem of calculating the inverse in $GF(2^8)$ can be translated to calculating the inverse in a smaller field. The multiplicative inverse of an arbitrary polynomial $b\boldsymbol{x} + c$ is given by:

$$(b\boldsymbol{x} + c)^{-1} = b(b^2\beta + bc\alpha + c^2)^{-1}\boldsymbol{x} + (c + b\alpha)(b^2\beta + bc\alpha + c^2)^{-1} \tag{5.3}$$

when the irreducible polynomial is $P(x) = x^2 + \alpha\boldsymbol{x} + \beta$ [61].

When Eq. 5.3 is applied recursively down to the base field $GF(2)$, the equation consists of operations which can be performed in the subfield $GF(2^m)$. The repeating degree-2 extensions are done using different irreducible polynomials listed in Tab. 5.1 [60]. By using this procedure, the multiplicative inverse operation may be implemented in hardware, as described in Sec. 5.4.2.

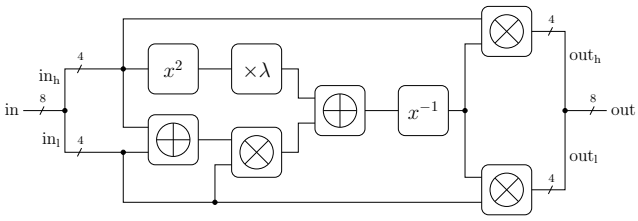


Figure 5.3: Multiplicative inverse, GF$(((2^2)^2)^2)$

5.3 Rijndael S-Box

The Rijndael S-box performs the SubBytes operations of the AES algorithm. The main operation of the S-box is to calculate the multiplicative inverse to a given 8-bit number over a finite field GF(2^8).

In most AES software implementations, the S-box is pre-generated into a look-up table, offering easy implementation and fast operation. This approach can also be taken when designing a hardware implementation, but such implementations are very area-demanding. By using composite field arithmetic a compact S-box with reduced computation cost may be realized [62]. Regardless of chosen solution, the S-box results in the biggest element in the AES algorithm.

5.3.1 S-Box Operation

The S-box function of an input byte a consists of the two following two transformations:

Inverse: The multiplicative inverse in the finite field GF(2^8) is calculated, $b = a^{-1}$. For the special case $a =$ 0x00, $b =$ 0x00.

Affine transformation: The following affine transformation is applied over GF(2):

$$b_i = a_i \oplus a_{(i+4)\text{mod}8} \oplus a_{(i+5)\text{mod}8} \oplus a_{(i+6)\text{mod}8} \oplus a_{(i+7)\text{mod}8} \oplus c_i \quad (5.4)$$

for $0 \leq i < 8$ where a_i is the i^{th} bit of the byte, and c_i is the i^{th} bit of a byte c with the value 01100011. The affine transformation element of

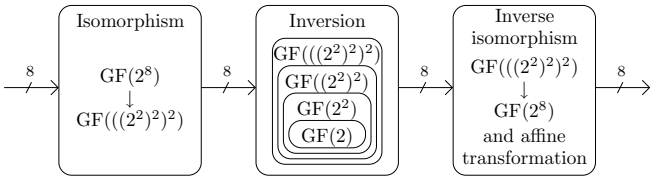


Figure 5.4: Implementation of the compact S-box

the S-box can be expressed in matrix form as:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

5.4 S-Box Circuit Implementation

Designing a compact S-box is one of the most critical challenges for reducing the total circuit size of the AES hardware [62]. A compact S-box reduces the power consumption significantly by reducing the number of gates. Large reduction in implementation area is obtained by using finite field arithmetic to reduce the fields order GF(2^8) to GF($(((2^2)^2)^2$) [62, 55, 60].

The S-box implementation selected is based on the implementation described by Satoh *et al.* [62], with the size optimization of Mentens *et al.* implemented [55].

As illustrated in Fig. 5.4, the compact S-box implementation consists of three stages:

Stage 1: Map all elements of the field A to a composite field B, using an isomorphism function δ.

Stage 2: Compute the multiplicative inverse over the field B.

Stage 3: Map all elements of the field B back to A, using the isomorphism function δ^{-1}.

5.4.1 Isomorphism, Inverse Isomorphism and Affine Transformation

The S-box implementation uses the isomorphism suggested by Mentens *et al.* in [55], which results in a small implementation. The isomorphic

mapping used is:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix}$$

where $a_i, b_i \in \mathrm{GF}(2)$ are the coefficients of $a \in \mathrm{GF}(2^8)$, $b \in \mathrm{GF}(((2^2)^2)^2)$. The resulting inverse transformation with affine transformation is:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

The corresponding irreducible polynomials are:

$$\begin{aligned} \mathrm{GF}(2^2): &\quad P(x) = x^2 + x + 1 \\ \mathrm{GF}((2^2)^2): &\quad P(y) = y^2 + y + \phi \\ \mathrm{GF}(((2^2)^2)^2): &\quad P(z) = z^2 + z + \lambda \end{aligned}$$

where $\phi = \{10\}_2$ and $\lambda = \{1100\}_2$.

Mappings and affine transformation are implemented by bit-addition using exclusive-OR gates. Schematic drawing of isomorphism from $\mathrm{GF}(2^8)$ to $\mathrm{GF}(((2^2)^2)^2)$ can be found in Sec. A.4.1. Inverse isomorphism and affine transformation are combined. The schematic drawing is shown in Sec. A.4.2.

5.4.2 Multiplicative Inverse Computation

By implementing Eq. 5.3 recursively down to $\mathrm{GF}(2)$ it is possible to implement the multiplicative inverse operation in hardware.

The multiplicative inverse cell is constructed of addition and multiplication cells. Addition in $\mathrm{GF}(2^n)$ is implemented by doing exclusive-OR of corresponding bits of two numbers. Implementation of multiplication is described below.

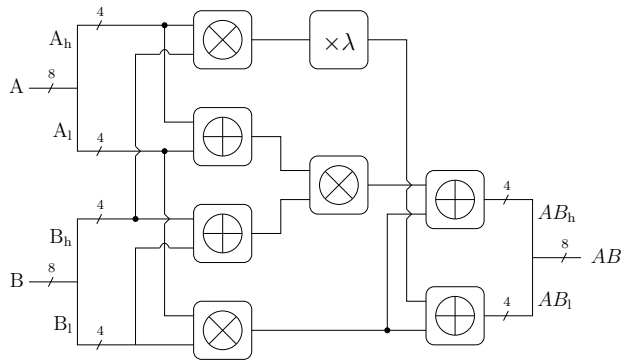


Figure 5.5: Multiplier $A \times B$, GF(2^8)

Multiplication

A Mastrovito composite field multiplier [60] is used to perform the multiplication. The multiplier may be represented as:

$$AB(x) = x((A_{\mathrm{L}} + A_{\mathrm{H}})(B_{\mathrm{L}} + B_{\mathrm{H}}) + A_{\mathrm{L}}B_{\mathrm{L}} + \lambda A_{\mathrm{H}}B_{\mathrm{H}} + A_{\mathrm{L}}B_{\mathrm{L}} \qquad (5.5)$$

where $A_{\mathrm{H}}, B_{\mathrm{H}}$ are the most significant half of the variables and $A_{\mathrm{L}}, B_{\mathrm{L}}$ are the least significant half of the variables. Circuit implementation is illustrated in Fig. 5.5, and is applied recursively using subfields of lesser degree to define the multipliers until the base field GF(2) is reached [60]. In GF(2), multiplication is implemented with the AND operation of the corresponding bits. The AND-gate is implemented as a NAND-gate followed by an inverter. The constant multiplication by λ is implemented as a circuit containing XOR gates.

5.4.3 Pipelining

Pipelining can be implemented for improving the throughput of the S-box. The S-box implementation is divided into four pipeline stages in the test setup in Paper IV. For optimal pipelining, the same amount of logic should be placed in every stage of the pipeline. The delay of each stage is estimated by counting elements in the longest datapath of each stage, as listed in Tab. 5.2.

The multiplicative inverse cell is separated into 3 stages for best distribution of calculation between the 4 pipeline stages. Latency of each stage is estimated and presented in Tab. 5.3. The delay of XOR and AND gates are estimated to 35 ns, and 40 ns for the overhead added by the flip-flop at 200 mV, and the corresponding clock period is set to 400 ns. At 1 V, the delays are set to 80 ps and 185 ps, respectively. The clock period at 1 V is set to 1 ns. Pipeline stages are inserted as illustrated in Fig. 5.6.

Table 5.2: Datapath gate count calculation

S-box stage	XOR-gates	AND-gates
Isomorphism	5	0
Multiplicative Inverse	18	4
Inverse Isomorphism and Affine Transformation	5	0

Table 5.3: Calculation of latency in pipeline

Stage	Cell	XOR-gates	AND-gates	Latency
1	Isomorphism	5	0	215 ns
2	Multiplicative Inverse	7	1	320 ns
3	Multiplicative Inverse	7	2	355 ns
4	Multiplicative Inverse, Inverse Isomorphism and Affine Transformation	9	1	390 ns

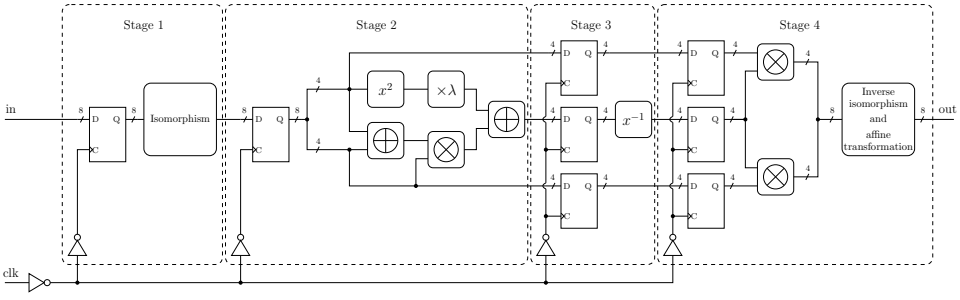


Figure 5.6: S-box pipeline stages

Chapter 6

Results

This chapter presents a brief overview of the outline and results from the papers included in this thesis.

6.1 Paper I

Seven Subthreshold Flip-Flop Cells

Outline: A comparative study of seven different flip-flop cells are performed with respect to metrics such as delay, power consumption, Power Delay Product and Energy Delay product. Flip-flops are important building blocks in many synchronous digital designs, as well as important parts of state machines. The seven considered flip-flop architectures are: (1) Basic Nand, (2) Transmission-gate Master-Slave (TGMS), (3) C^2MOS, (4) PowerPC 603, (5) True Single-Phase Clock (TSPC), (6) Dynamic TGMS, (7) Dynamic C^2MOS.

Results: All flip-flop cells are simulated with respect to the power supply voltage in the region of 150 mV to 350 mV. The output waveform indicates that all flip-flop cells are able to operate with a power supply voltage in the given region. Power consumption is measured with an operating frequency of 1 MHz.

Operating at a power supply voltage of 150 mV, an average power dissipation of 165.5 pW was achieved for a dynamic and 285 pW for a static flip-flop topology.

6.2 Paper II

Three Subthreshold Flip-Flop Cells Characterized in 65 nm and 90 nm CMOS Technology

Outline: Three flip-flop designs, selected from the results of [63] and [18], are simulated with a power supply voltage ranging from 125 mV to 1 V. These flip-flop designs are: (1) PowerPC 603, (2) Sense-amplifier based flip-flop (SAFF) and (3) Dynamic C^2MOS. In addition to metrics simulated in [63], process variations are taken into account by simulation at different process corners. Simulation in 65 nm process is done in addition to 90 nm.

Results: Simulation results of all flip-flops are shown, measured as total delay, average power consumption, Power-Delay Product and Energy-Delay Product with respect to power supply voltage. Performance of all flip-flops in TT, FF, SS, FS and SF process corners is shown regarding delay and power consumption at 150 mV and 1 V. The relationship between the FF and SS process corners are calculated with respect to power supply voltage. Numbers of successful corners in subthreshold region for all flip-flops are shown. Improvement factor for delay, power consumption, PDP and EDP metrics are calculated for the PowerPC 603 flip-flop running with power supply voltage of 125 mV comparing to 1 V. Power consumption is measured at maximum operating frequency.

With a reduction of the supply voltage from 1 V to 125 mV, the power consumption of a single flip-flop cell is reduced with a factor of 20 000.

6.3 Paper III

Improving Circuit Security against Power Analysis Attacks with Subthreshold Operation

Outline: Power analysis attacks have emerged as a major security threat in the area of secure ICs. A comparison between input data and instantaneous power consumption is done with a power supply voltage of 200 mV and 1 V for a 8 bit full adder.

Results: The correlation between the input data and the power consumption is calculated by running 1 000 transient simulations on the full adder with random input combinations. Power consumption is measured as current drawn from the power supply voltage. A maximum current of 650 μA is measured in superthreshold operation, while a maximum current of 0.41 μA is measured in subthreshold operation. The correlation is measured by

calculating the standard deviation of the current drawn from the power supply voltage of the 1 000 different transient simulations. This standard deviation is normalized, and a standard deviation of 1.0 is the maximum in superthreshold operation. At subthreshold operation the maximum standard deviation is 0.00052, which is a decrease of approximately 1 900 times. The power consumption correlation is reduced at the cost of 600 times delay time degradation.

6.4 Paper IV

Subthreshold AES S-Box with Increased Power Analysis Resistance

Outline: A compact AES S-box is implemented and tested for power analysis resistance in subthreshold operation compared to superthreshold operation. The S-Box operation is one of the major building blocks of the AES algorithm. Resistance against Differential Power Analysis (DPA) attacks is measured by calculating the correlation in the instantaneous supply current when different input vectors are applied. The S-box is implemented in an asynchronous version, as well as a pipelined version for increased throughput.

Results: All 256 input combinations are simulated with a supply voltage of 200 mV and 1 V. The supply current drawn from V_{DD} and the calculation time used is stored for each input.

The standard deviation is calculated and normalized, as in Paper III. While the normalized standard deviation for the asynchronous S-box is 1.0 at V_{DD} = 1 V, it is reduced to 0.00040 at 200 mV. This corresponds to a reduction in the correlation between data being processed and the power consumption with a factor 2 500, while the calculation time increases 350 times.

The throughput of the S-box is increased from 7.37 Mbits to 19.88 Mbits at V_{DD} = 200 mV when 4 pipeline stages are introduced. The same factor of decrease in correlation and increase in calculation time is obtained in the pipelined S-box.

The calculation time, power consumption, PDP and EDP metrics for the asynchronous S-box are measured when the supply voltage is stepped up from 125 mV to 1 V. The lowest PDP value, 68.8 fJ, is obtained with $V_{DD} = 250$ mV. The lowest EDP value is obtained when running at 750 mV, and it is 1.36 zJs.

Chapter 7

Discussion

7.1 Minimizing Power Consumption

CMOS technology stands above enormous challenges in managing the increased power consumption in modern and future deep submicron CMOS devices. Subthreshold operation is an effective mean for reducing the power consumption dramatically by using existing CMOS technology without the need for major change in system design. In combination with massive parallelism and pipelining it may be possible to maintain high performance and throughput while running in the subthreshold regime [64].

Through simulations presented in Paper I, II, III and IV it is shown that significant reduction in power consumption is achieved by reducing the power supply voltage. For certain applications requiring very low power consumption subthreshold operation is presented as a promising alternative to conventional CMOS operation. The gate delays increase when the supply voltage is scaled down since capacitances and threshold voltage are constant [65]. High performance application may therefore presently not be suitable for subthreshold operation.

For most sequential circuit systems, subthreshold supply voltage does not offer the lowest possible energy per cycle. As seen in PDP and EDP plots in included papers, minimum values are often obtained with a supply voltage somewhere in between the subthreshold region and the nominal voltage of the process. For example, the best PDP and EDP values for the S-box in Paper IV are obtained with a supply voltage of 250 mV and 750 mV, respectively. The supply voltage offering minimum energy consumption per cycle depends on the technology, the characteristics of the cycle, and workload of the system [14]. Careful analysis of optimum supply voltage should therefore be done for each design, depending on its performance goal.

Simulation results in Paper I and II show that sequencing elements,

represented by flip-flops, operate well when power supply voltage is scaled down into the subthreshold region.

In Paper III, subthreshold operation reduces the power consumption on an arithmetic 8-bit function. The power consumption is reduced significantly in a cryptographic function with and without sequencing elements, as shown in Paper IV.

7.2 Process Variations

Subthreshold circuits are more sensitive to process variations compared to conventional circuits. Threshold voltage in modern processes varies with process variations, which leads to increased variations in circuit performance and reduced yield if threshold voltages do not match. Body-bias regulation can be used to decrease the variation of V_t and increase the yield [38].

Dynamic designs are more sensitive to leakage currents than static designs, and especially the gate leakage current. Due to reduced I_{on}/I_{off} ratio in subthreshold operation, dynamic designs are more sensitive to process variations. Simulation results in Paper II confirm that dynamic designs are sensitive to process variations and require a higher operation voltage to operate successfully in all corners.

Accurate technology models are required for realistic simulations in the simulation environment. By simulating on the schematic, parameters depending on the physical layout of the design cannot be modelled accurately. For example, interconnect capacitance and parasitic effects depend on length of wires and other selections done in the physical layout. Previous experience at the research group [1] with STMicroelectronics' 90 nm process indicate good compliance between schematic simulations and actual performance of produced circuits. Presently, compliance between model and actual performance of produced circuits in the 65 nm process has not been tested at the group. It would be instructive to produce test circuits for verifying the model's accuracy. However, the 65 nm process has only been used in Paper II for comparing with the 90 nm process and it has not been considered to be the subject of this thesis to validate the process model. Since the research group has good experience with the 90 nm process, it has been used through Paper III and IV. Due to restricted project time, layout simulations were not prioritized in this project.

Statistical Monte Carlo simulations would be instructive for in-depth examination of yield numbers. However, the total circuit yield is often more dependent on other circuit elements than flip-flop, as flip-flops are an integrated part of a larger circuit. For best results, flip-flops performing successfully in all corners at the desired supply voltage should be chosen

[1] Nanoelectronic Research Group, Dept. of Informatics, Univ. of Oslo

in implementations. Simulation results indicate that the PowerPC 603 flip-flop has the highest tolerance against process variations at low voltages and operates successfully in all corners at 125 mV.

Correct functionality is crucial as many customers have requirements down to 1-2 Defect Parts per Million (DPPM). Small defect tolerance requires not only high yield numbers, but also a good testing environment for manufactured devices. Testing may be difficult in subthreshold region. For example, detecting faulty parts by looking at the quiescent background current may be difficult, as the I_{on}/I_{off} ratio is significantly reduced.

7.3 Power Analysis Attack Resistance

Power analysis attacks have recently gained scientific research interest as the market for secure ICs has increased. Due to the increased use of modern electronic communication systems, secure handling of data has become of great concern when designing secure ICs.

In modern cryptographic systems, secure against known mathematical cryptoanalysis attacks, side-channel attacks emerge as a major security threat. The AES algorithm is secure against known cryptoanalytic methods, and the only known form of attacks on the AES algorithm presently are side-channel attacks [45]. Cryptographic circuits must be designed with minimization of side-channel leakage in mind.

Simulations in Paper III and IV have focused on the powerful DPA attack. Power consumption of circuits with a wide range of different input vectors is compared, and the standard deviation is calculated. DPA attacks are harder to perform with a decreased standard deviation [5].

Research on the countermeasure effect of operating transistors in the subthreshold region has so far almost been lacking, even though this is one of the best known methods for decreasing both the signal magnitude and the signal-noise ratio. Operating in subthreshold region also involves minimizing the dynamic power consumption component of the total power consumption, and therefore making the power consumption less correlated to switching activity of circuitry.

By running a cryptographic IC in subthreshold operation, an increased security against power analysis attacks is obtained by the simulation results. Although subthreshold operation offers increased resistance against power analysis attacks, circuits are not fully protected against attacks as long as there exists some correlation between the processed data and the instantaneous supply current [66]. Subthreshold operation should be considered implemented together with other DPA countermeasure techniques for improved resistance. Promising reported techniques worth mentioning include differential masking, random noise addition and blinding [66, 49, 8].

Discussion

Subthreshold operation leads to an increased execution time, which may not be acceptable for high-performance implementation in high-speed communication systems. In many low-power systems, such as sensor networks, subthreshold operation offers both decreased power consumption and increased resistance against side-channel attacks.

Chapter 8

Conclusion

The International Technology Roadmap for Semiconductors regards power management as the primary issue across most CMOS application segments presently [1]. Subthreshold operation is the most dramatic way to obtain a necessary reduction in power consumption.

Through four papers simulation results on subthreshold performance of both sequencing and combinational logic are presented, as well as a complete pipelined S-Box system implemented with a combination of these VLSI gate families.

Simulation results indicate, in addition to published works from other authors, that subthreshold operation is a promising method for designing future CMOS systems with strict power consumption requirements.

In general, the simulation results show that the 65 nm process offers lower delay time but higher power consumption compared to the 90 nm process.

Paper I examines seven commonly used flip-flop cells in subthreshold operation. With an operating frequency of 1 MHz a delay of 77.9 ns and a power consumption of 165.5 pW are achieved for the dynamic C^2MOS flip-flop at 150 mV. The PowerPC 603 flip-flop offers both the best delay time and power consumption of the static topologies, with $t_{\text{delay}} = 120$ ns and a power consumption of 285 pW at 150 mV.

In Paper II, further examinations are done on three flip-flop cells, with process corner's performance and two CMOS processes taken into account. According to the simulation results, the PowerPC 603 flip-flop in the 65 nm process offers the best delay time $t_{\text{delay}} = 28.7$ ns with a power supply voltage of 125 mV, while the Sense-Amplifier based Flip-Flop (SAFF) in the 90 nm process offers the lowest power consumption $P_{\text{avg}} = 256$ pW at $V_{\text{DD}} = 125$ mV. Flip-flop simulations at different process corners are taken into account. These simulations indicate that flip-flops are able to operate in most process corners at very low supply voltages without malfunctioning. The simulation results indicate that the PowerPC 603

flip-flop design would be the most suitable choice of design for ultra-low-voltage operation, as it operates successfully in all process corners at 125 mV in the 65 nm process.

Side-channel attacks emerge as a major security threat in modern cryptographic systems. Cryptographic circuit designing must be done with minimization of side-channel information leakage in mind. Paper III and IV demonstrate the increased power analysis attack resistance achieved by running in the subthreshold regime. As indicated by simulations, standard CMOS logic operated in the subthreshold region provides orders of magnitude increased resistance against power analysis attacks.

Simulations on an 8 bit full adder in Paper III show that subthreshold operation reduces the correlation between data being processed and the power consumption with a factor of 1 900, compared to nominal superthreshold operation.

In Paper IV, a compact AES S-box running in the subthreshold regime is presented. The simulation results indicate an increased resistance against power analysis attacks, as the correlation factor is reduced 2 500 times. Increased throughput is obtained by implementing a 4 stage pipeline.

As explored in this thesis, subthreshold operation emerges as a promising mean for coping with the increased power dissipation in modern CMOS processes. Results from Paper III and IV present subthreshold operation for increased resistance against power analysis attacks. Subthreshold operation arises as a promising operation mode for today's and future's low power CMOS circuits.

8.1 Future work

This thesis has touched into some aspects of the large and complex field of digital subthreshold operation. The potential of further works in the field is large, and some suggestions for future works are listed below:

- As subthreshold circuits are sensitive to process variations, deeper analysis of process variations effect on power consumption and delay time would be instructive. Simulations with temperature variations on the overall subthreshold process variation robustness would be of great interest. Similarly, Monte Carlo simulations on a complete subthreshold system, such as the S-box, would be instructive for estimating process variations.

- Body-bias regulation has been suggested as a solution for coping with the increased process variation sensitivity. Several works with promising results have been published. Analyzing expected yield improvements in a subthreshold increased DPA resistant circuit with body-bias regulation would be of interest. The AES S-box design

implemented in Paper IV has potential for further optimizations at the logic level using digital synthesize tools. Such tools can optimize logic functions and replace some of the AND gates with NAND gates for reducing area and power consumption [67]. Subthreshold operation should be considered implemented together with other countermeasure techniques for making cryptographic circuits more resistant against side-channel attacks.

- To be able to test and confirm key points in this thesis, a chip implementation of a complete AES system could be produced. The optimal goal would be to construct a complete subthreshold AES chip with body-bias regulation implemented, as well as other proposed DPA techniques. Due to limited project time, this was not possible to do in the scope of this thesis.

Chapter 9

Acronyms

AES Advanced Encryption Standard

CMOS Complementary Metal-Oxide Semiconductor

DES Data Encryption Standard

DPA Differential Power Analysis

DPPM Defect Parts per Million

EDP Energy-Delay Product

EMA Electromagnetic Analysis

FIPS Federal Information Processing Standard

HLFF Hybrid Latch Flip-Flop

IC Integrated Circuit

MOSFET Metal-Oxide-Semiconductor Field-Effect Transistor

NIST National Institute of Standard and Technology

nMOS N-channel MOSFET

PDP Power-Delay Product

pMOS P-channel MOSFET

SAFF Sense-Amplifier based Flip-Flop

S-box Substitution box

SDFF Semi-Dynamic Flip-Flop

SPA Simple Power Analysis

Acronyms

TGMS Transmission-gate Master-Slave Flip-Flop

TSPC True Single-Phase-Clock Flip-Flop

VLSI Very Large Scale Integrated Circuit

Appendix A

Schematic Drawings and Transistor Sizing

In this chapter the different design for all simulations are presented as schematic drawings, including transistor sizes.

A.1 Basic Logic Functions

A.1.1 Inverter

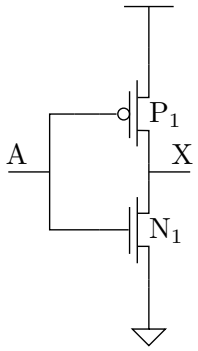


Figure A.1.1: Inverter schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_1	0.36	0.1
N_1	0.12	0.1

A.1.2 NAND

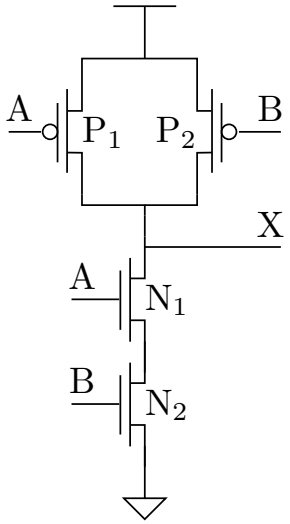


Figure A.1.2: NAND schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_{1-2}	0.24	0.1
N_{1-2}	0.12	0.1

A.1.3 XOR

Complementary CMOS XOR design

This C^{2}MOS based XOR design is used in the S-box implementation.

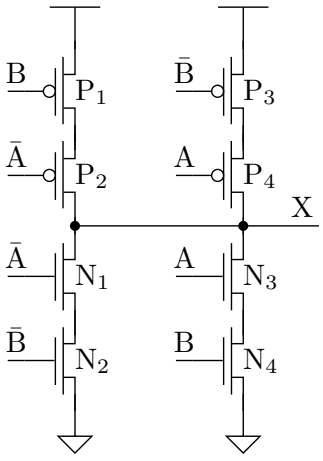


Figure A.1.3: C^{2}MOS XOR schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_{1-4}	0.48	0.1
N_{1-4}	0.24	0.1

Tiny-XOR design

The tiny-XOR design offers a small XOR implementation. This design was used in the implementation of 1 bit half-adder.

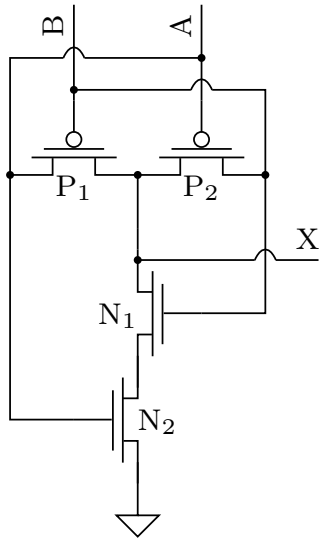


Figure A.1.3: Tiny XOR schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_1	0.12	0.1
P_2	0.12	0.1
N_1	0.12	0.1
N_2	0.12	0.1

A.2 Flip-Flops

A.2.1 NAND-Master-Slave Flip-Flop

The basic NAND flip-flop is constructed out of NAND-gates. Each NAND-based latch requires a total 16 transistors.

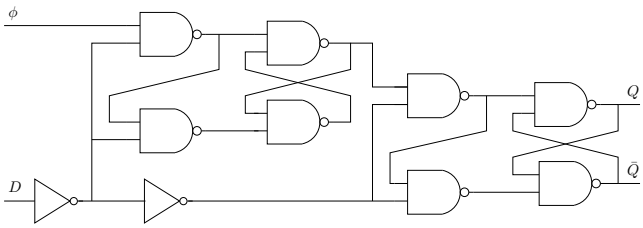


Figure A.2.1: NAND-MS flip-flop schematic

A.2.2 Transmission Gate Master Slave Flip-Flop

The Transmission Gate Master Slave (TGMS) flip-flop uses clocked transmission gates.

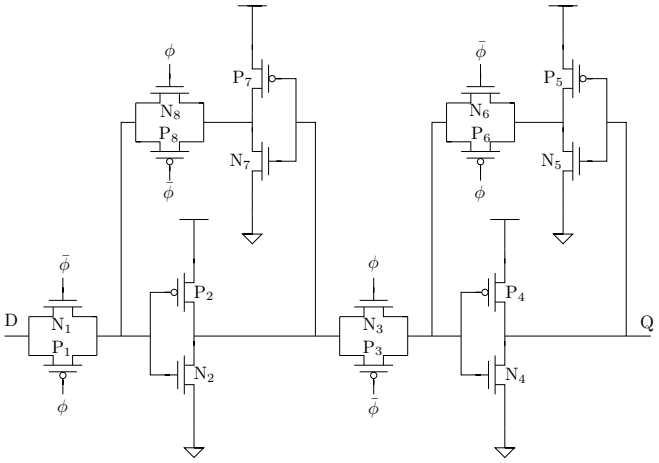


Figure A.2.2: TGMS flip-flop schematic

Transistor	$W_{90\,\mathrm{nm}}$ (nm)	$L_{90\,\mathrm{nm}}$ (nm)
P_{1-8}	0.36	0.2
N_{1-8}	0.24	0.2

A.2.3 C^{2}MOS Flip-Flop

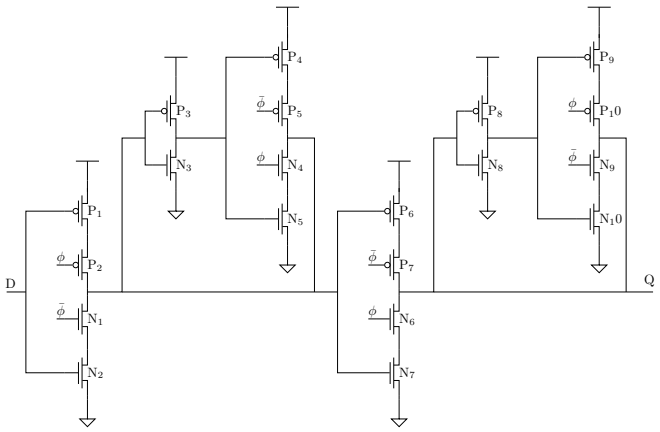


Figure A.2.3: C^{2}MOS flip-flop schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_{1-10}	0.36	0.2
N_{1-10}	0.24	0.2

A.2.4 PowerPC 603 Flip-Flop

The PowerPC 603 flip-flop was used in the PowerPC 603 microprocessor. It is a combination of the TGMS and C^{2}MOS flip-flop designs.

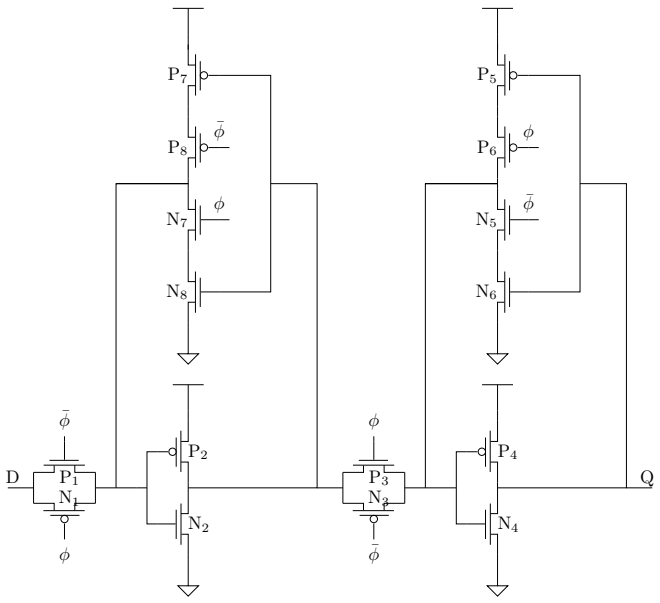


Figure A.2.4: PowerPC 603 flip-flop schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)	$W_{65\,\mathrm{nm}}$ (μm)	$L_{65\,\mathrm{nm}}$ (μm)
P_{1-8}	0.36	0.1	0.12	0.06
N_{1-8}	0.12	0.1	0.18	0.06

A.2.5 TSPC Flip-Flop

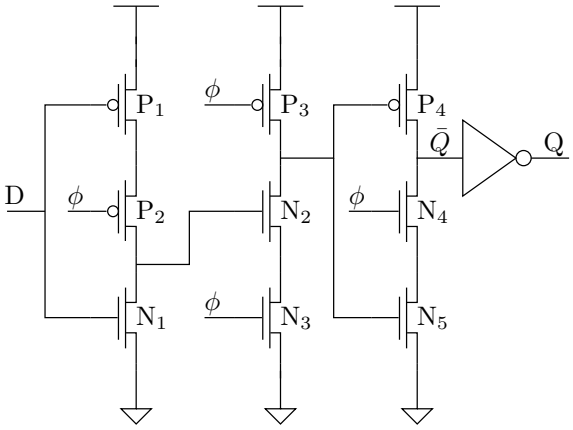


Figure A.2.5: TSPC flip-flop schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_1	0.585	0.1
P_2	0.585	0.1
P_3	0.12	0.1
P_4	0.24	0.1
N_1	0.12	0.1
N_2	0.27	0.1
N_3	0.27	0.1
N_4	0.54	0.1
N_5	0.54	0.1

A.2.6 Dynamic TGMS Flip-Flop

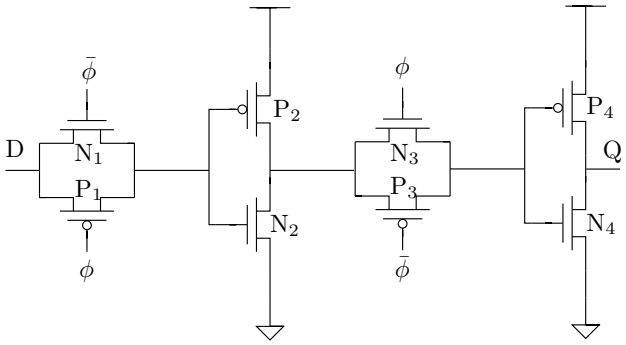


Figure A.2.6: Dynamic TGMS flip-flop

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_1	0.12	0.2
P_2	0.36	0.2
P_3	0.12	0.2
P_4	0.36	0.2
N_1	0.24	0.2
N_2	0.24	0.2
N_3	0.24	0.2
N_4	0.24	0.2

A.2.7 Dynamic C^{2}MOS Flip-Flop

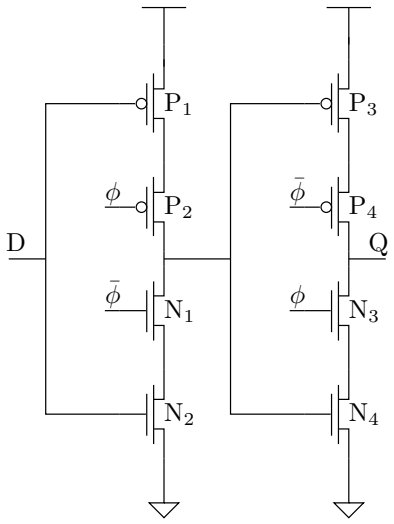


Figure A.2.7: Dynamic C^{2}MOS flip-flop

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)	$W_{65\,\mathrm{nm}}$ (μm)	$L_{65\,\mathrm{nm}}$ (μm)
P_{1-4}	0.36	0.1	0.12	0.12
N_{1-4}	0.12	0.1	0.24	0.12
P_{inv}	0.36	0.1	0.12	0.12
N_{inv}	0.12	0.1	0.24	0.12

A.2.8 Sense-Amplifier Based Flip-Flop

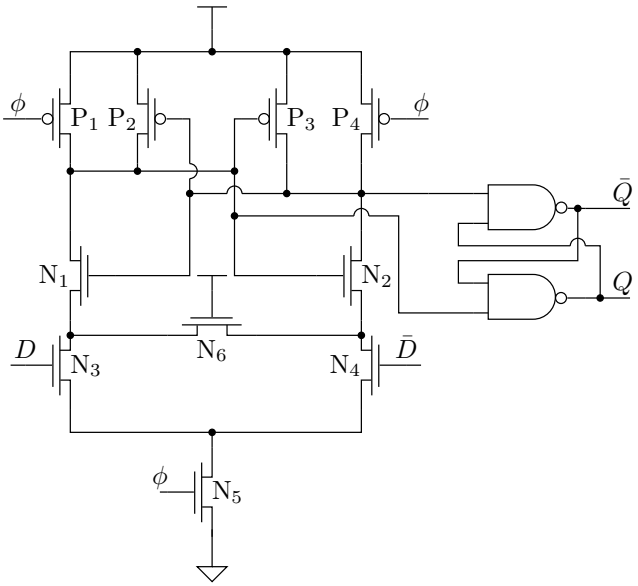


Figure A.2.8: Sense-Amplifier Based flip-flop

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)	$W_{65\,\mathrm{nm}}$ (μm)	$L_{65\,\mathrm{nm}}$ (μm)
P_{1-4}	0.12	0.1	0.36	0.06
N_{1-6}	0.12	0.1	0.12	0.06

A.3 Full-Adder

A.3.1 1 Bit Half-Adder

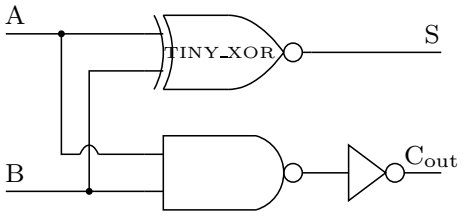


Figure A.3.1: 1 bit half-adder schematic

A.3.2 1 Bit Full-Adder

The 1 bit full-adder cell presented in [68]. The same transistor sizing has been used.

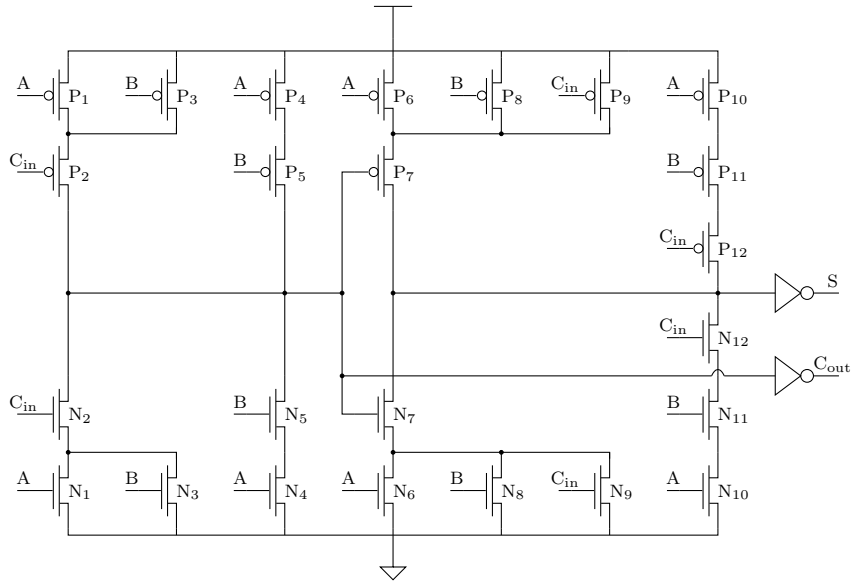


Figure A.3.2: 1 bit full-adder schematic

Transistor	$W_{90\,\mathrm{nm}}$ (μm)	$L_{90\,\mathrm{nm}}$ (μm)
P_{1-12}	0.4	0.1
N_{1-12}	0.2	0.1

A.3.3 8 Bit Full-Adder

The 8 bit full-adder is constructed as a ripple-adder. A half-adder is used for the first bit, while full-adders are used for all other bits.

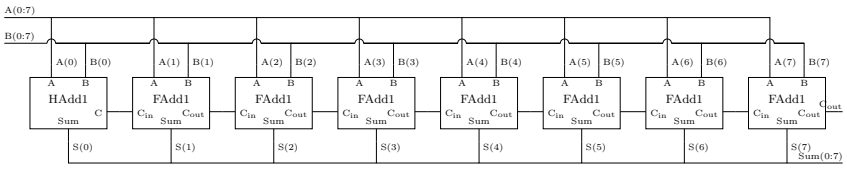


Figure A.3.3: 8 bit full-adder schematic

A.4 S-box

A.4.1 Isomorphism

The isomorphism (mapping from GF(2^8) to GF($((2^2)^2)^2$)) is implemented with exclusive-OR addition as described in Sec. 5.4.1.

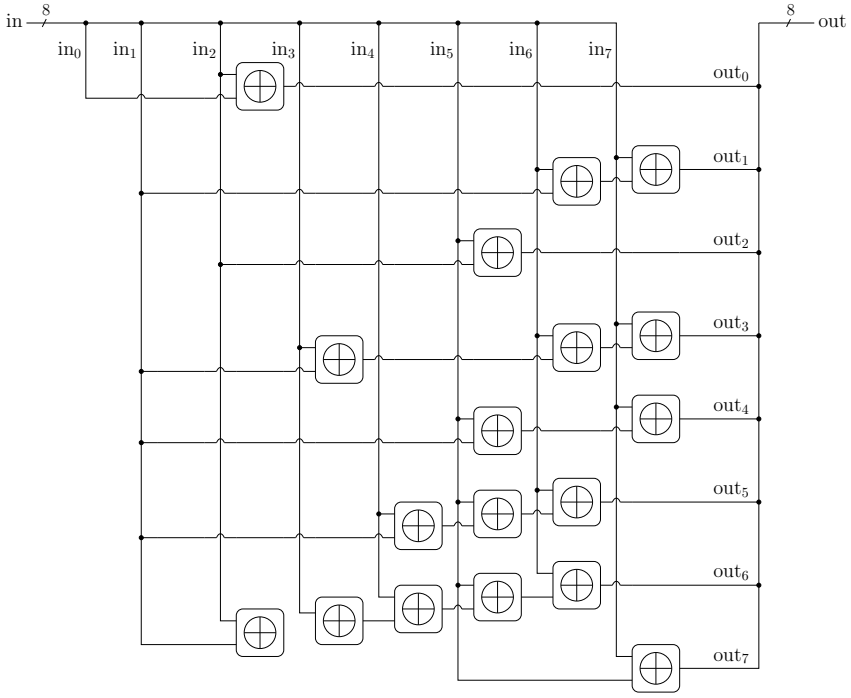


Figure A.4.1: S-box Isomorphism Cell

A.4.2 Inverse Isomorphism and Affine Transformation

The inverse isomorphism (mapping from GF($((2^2)^2)^2$) to GF(2^8)) and affine transformation is implemented with exclusive-OR addition as described in Sec. 5.4.1.

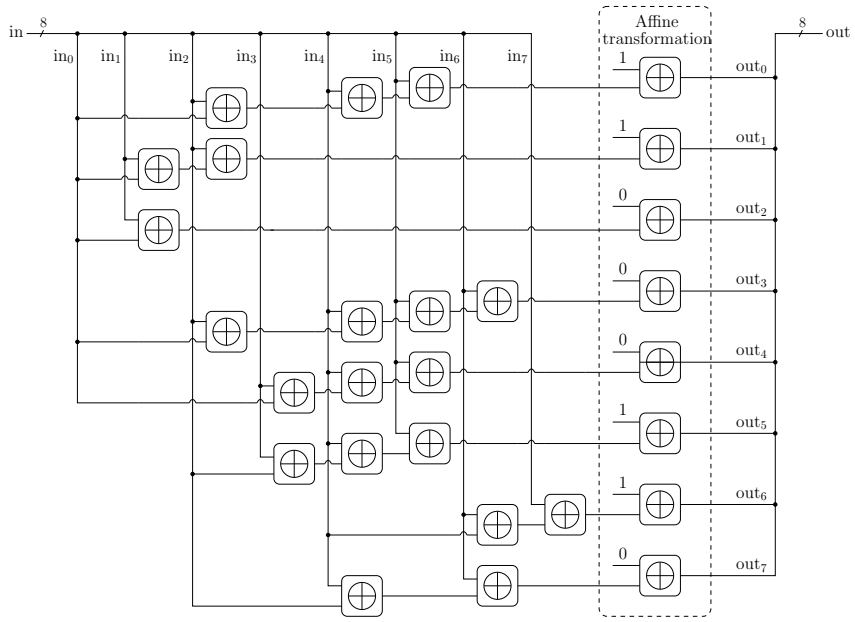


Figure A.4.2: S-box Inverse Isomorphism and Affine Transformation cell

Appendix B

Additional Simulations

B.1 Subthreshold Transistor Sizing

Parametric simulations on the effect of sizing in the subthreshold region have been done on a selection of circuit elements. The simulations have made the basis for decisions done on transistor dimensioning during the thesis. The simulations have been done with respect to delay and power consumption.

B.1.1 Inverter

As shown in Fig. B.1, an inverter is simulated with different nMOS and pMOS width ranging from 0.12 μm (minimum size) to 0.40 μm in the 65 nm process with V_{DD} = 150 mV.

Simulation results indicates best delay time with W_p = 0.12 μm and W_n = 0.14 μm. The power consumption is lowest when W_n is minimum sized but seems to be relative independent of the pMOS width.

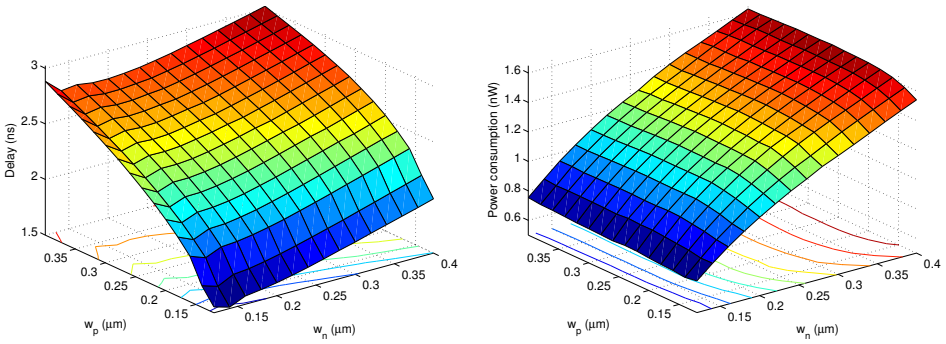
B.1.2 PowerPC 603

The PowerPC 603 flip-flop is simulated with the same test setup as the inverter. The simulation result is plotted in Fig. B.2. All pMOS and all nMOS transistors are set to the same width.

The lowest delay time is achieved with the same sizing as in the inverter's case. With W_p = 0.24 μm and W_n = 0.12 μm the lowest average power consumption is obtained.

B.1.3 NAND

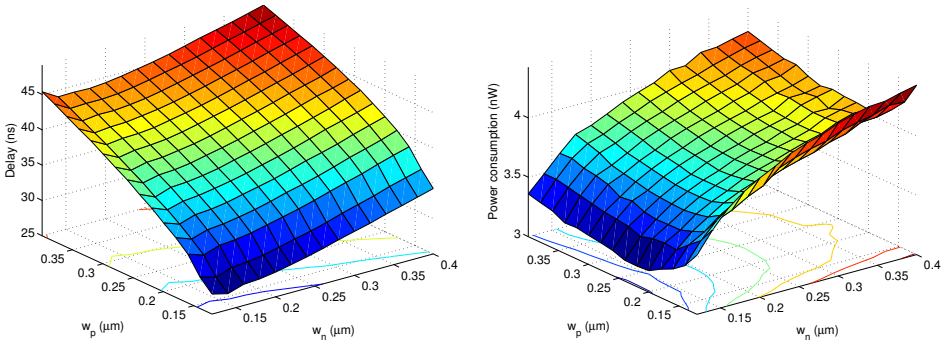
A NAND-gate is simulated in the 90 nm process at V_{DD} = 200 mV with respect to delay time. The simulation results are plotted in Fig. B.3. In Fig. B.3(b), delay time in all process corners are simulated.



(a) Inverter delay

(b) Inverter power consumption

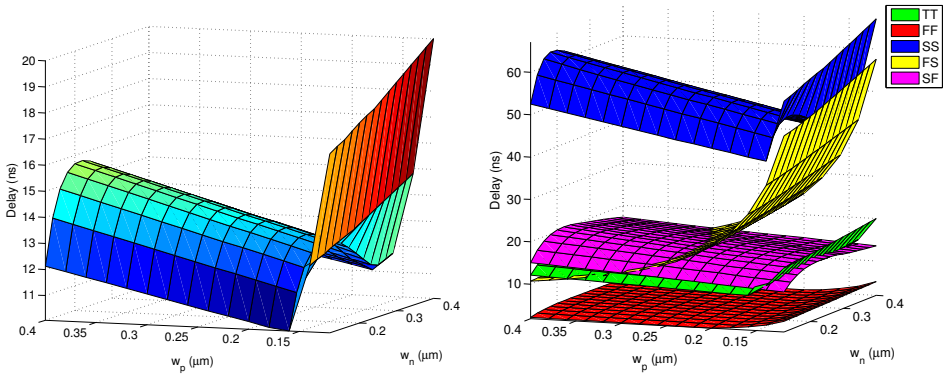
Figure B.1: Effect of transistor sizing in subthreshold on an inverter



(a) PowerPC 603 delay

(b) PowerPC 603 power consumption

Figure B.2: Effect of transistor sizing in subthreshold on the PowerPC 603 flip-flop



(a) NAND delay

(b) NAND process corners delay

Figure B.3: Effect of transistor sizing in subthreshold on a NAND-gate

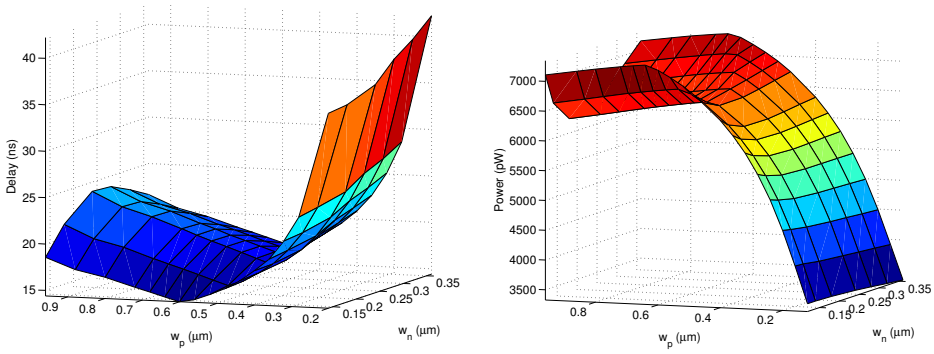
From the simulation it can be observed that minimum pMOS width results in a large delay compared to a small increase in pMOS width. For implementation, $W_n = 0.12\,\mu$m and $W_p = 0.16\,\mu$m are chosen.

B.1.4 C^{2}MOS XOR

The C^{2}MOS XOR-gate (see Sec. A.1.3) is simulated in the 90 nm process at $V_{DD} = 200$ mV with respect to delay time and power consumption, and plotted in Fig. B.4. The best delay time is achieved when $W_n = 0.12\,\mu$m and $W_p = 0.6\,\mu$m according to the simulation results, but such sizing results in high power consumption.

B.2 S-Box Output

The S-box implemented in Paper IV has been tested to give valid output for all input combinations, according to FIPS 197 [56]. The output produced by the S-box implementation is listed in Tab. B.1.



(a) C^2MOS XOR delay

(b) C^2MOS XOR power consumption

Figure B.4: Effect of transistor sizing in subthreshold on the C^2MOS XOR-gate

Table B.1: S-box simulated output values (in hexadecimal form)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Bibliography

[1] (2007, Dec.) International technology roadmap for semiconductors, executive summary 2007. [Online]. Available: http://www.itrs.net/

[2] (2008, Feb.) Intel fact sheet - fun facts: Excactly how small (and powerful) is 45 nanometers. [Online]. Available: http://www.intel.com/pressroom/kits/45nm/

[3] G. Moore, "Cramming more components onto integrated circuits," *Electronics*, vol. 38, no. 8, pp. 114–117, 1965.

[4] G. Schrom and S. Selberherr, "Ultra-low-power CMOS technologies," in *Proc. of IEEE International Semiconductor Conference (CAS'96)*, Oct. 1996, pp. 237–246.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. of International Cryptology Conference on Advances in Cryptology (CRYPTO'99)*, ser. Lecture Notes in Computer Science, vol. 1666. Springer, 1999, pp. 388–397.

[6] J.-S. Coron, P. Kocher, and D. Naccache, "Statistics and secret leakage," *ACM Transactions on Embedded Computing Systems*, vol. 1962, pp. 157–173, Feb. 2001.

[7] J. Fournier and M. Tunstall, "Cache based power analysis attacks on AES," in *Proc. of Australasian Conference on Information Security and Privacy*, ser. Lecture Notes in Computer Science, vol. 4058. Springer, 2006, pp. 17–28.

[8] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, pp. 1197–1208, July 2006.

[9] J. Rabaey, M. Pedram, and P. Landman, *Low Power Design Methodologies*. Boston: Kluwer Academic Publishers, 1995.

[10] F. Leuenberger and E. Vittoz, "Complementary-MOS low-power low-voltage integrated binary counter," in *Proc. of the IEEE*, vol. 57, no. 9, Sept. 1969, pp. 1528–1532.

[11] R. M. Swanson and J. D. Meindl, "Ion-implanted complementary MOS transistors in low-voltage circuits," *IEEE Journal of Solid-State Circuits*, vol. 7, pp. 146–153, Apr. 1972.

[12] J. B. Burr and J. Shott, "A 200mV self-testing encoder/decoder using standford ultra-low-power CMOS," in *Proc. of IEEE International Solid-State Circuits Conference (ISSCC'94)*, Feb. 1994, pp. 84–85.

[13] B. H. Calhoun and A. Chandrakasan, "Characterizing and modeling minimum energy operation for subthreshold circuits," in *Proc. of IEEE International Symposium on Low Power Electronics and Design Conference (ISPLED'04)*, Newport Beach, CA, USA, Aug. 2004, pp. 90–95.

[14] B. H. Calhoun, A. Wang, and A. Chandrakasan, "Modeling and sizing for minimum energy operation in subthreshold circuits," *IEEE Journal of Solid-State Circuits*, vol. 40, pp. 1778–1786, Sept. 2005.

[15] A. Wang and A. Chandrakasan, "A 180 mV subthreshold FFT processor using a minimum energy design methodology," *IEEE Journal of Solid-State Circuits*, vol. 40, pp. 310–319, Jan. 2005.

[16] B. C. Paul, A. Raychowdhury, and K. Roy, "Device optimization for digital subthreshold logic operation," *IEEE Transactions on Electron Devices*, vol. 52, pp. 237–247, Feb. 2005.

[17] H. Soeleman, K. Roy, and B. C. Paul, "Robust subthreshold logic for ultra-low power operation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 9, pp. 90–99, Feb. 2001.

[18] B. Fu and P. Ampadu, "Comparative analysis of ultra-low voltage flip-flops for energy efficiency," in *Proc. of IEEE Circuits and Systems (ISCAS'07)*, New Orleans, USA, May 2007, pp. 1173–1176.

[19] J. Chen, L. T. Clark, and T.-H. Chen, "An ultra-low-power memory with a subthreshold power supply voltage," *IEEE Journal of Solid-State Circuits*, vol. 41, pp. 2344–2353, Oct. 2006.

[20] P. Ampadu, "Ultra-low voltage VLSI: Are we there yet?" in *Proc. of IEEE International Symposium on Circuits and Systems (ISCAS'06)*, May 2006, pp. 21–24.

[21] J. P. Kulkarni, K. Kim, and K. Roy, "A 160 mV robust schmitt trigger based subthreshold SRAM," *IEEE Journal of Solid-State Circuits*, vol. 42, pp. 2303–2313, Oct. 2007.

[22] A. Argarwal, N. Banerjee, S. K. Hsu, R. K. Krishnamurthy, and K. Roy, "A 200mV to 1.2V, 4.4MHz to 6.3GHz, 48x42b 1R/1W programmable register file in 65nm CMOS," in *Proc. of IEEE European Solid State*

Circuits Conference (ESSCIRC'07), Munich, Germany, Sept. 2007, pp. 316–319.

[23] S. Hanson, B. Zhai, M. Seok, B. Cline, K. Zhou, M. Singhal, M. Minuth, J. Olson, L. Nazhandali, T. Austin, D. Sylvester, and D. Blaauw, "Exploring variability and performance in a sub-200-mV processor," *IEEE Journal of Solid-State Circuits*, vol. 43, pp. 881–891, Apr. 2008.

[24] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. of International Cryptology Conference on Advances in Cryptology (CRYPTO'97)*, ser. Lecture Notes in Computer Science, vol. 1109. Springer, Aug. 1996, pp. 104–113.

[25] D. Liu and C. Svensson, "Trading speed for low power by choise of supply and threshold voltages," *IEEE Journal of Solid-State Circuits*, vol. 28, pp. 10–17, Jan. 1993.

[26] A. G. Andreou, , K. A. Boahen, P. O. Pouliquen, A. Pavasović, R. E. Jenkins, and K. Strohbehn, "Current-mode subthreshold MOS circuits for analog VLSI neural systems," *IEEE Transactions on Neural Networks*, vol. 2, pp. 205–213, Mar. 1991.

[27] H. Soeleman and K. Roy, "Ultra-low power digital subthreshold logic circuits," in *Proc. of IEEE International Symposium on Low Power Electronics and Design (ISPLED'99)*, Aug. 1999, pp. 94–96.

[28] L. Nazhandali, B. Zhai, J. Olson, A. Reeves, M. Minuth, R. Helfand, S. Pant, T. Austin, and D. Blaauw, "Energy optimization of subthreshold-voltage sensor network processors," in *Proc. of IEEE International Symposium on Computer Architecture (ISCA'05)*, Madison, WI, USA, June 2005, pp. 197–207.

[29] N. H. E. Weste and D. Harris, *CMOS VLSI Design - A Circuits and Systems Perspective*. Boston, MA: Addison-Wesley, 2005.

[30] K. Roy, S. Mukhopadhyay, and H. Mahmoodi-Meimand, "Leakage current mechanisms and leakage reduction techniques in deep-submicrometer CMOS circuits," pp. 305–327, Feb. 2003.

[31] S. Xue and B. Oelmann, "Comparative study of low-voltage performance of standard-cell flip-flops," in *Proc. of IEEE International Conference on Electronics, Circuits, and Systems (ICECS'01)*, vol. 2, Malta, 2001, pp. 953–957.

[32] X. Qi, S. C. Lo, A. Gyure, Y. Luo, M. Shahram, K. Singhal, and D. B. MacMillen, "Efficient subthreshold leakage current optimization," *IEEE Circuits and Devices Magazine*, vol. 5, pp. 39–47, 2006.

[33] E. J. Nowak, "Maintaining the benefits of CMOS scaling when scaling bogs down," *IBM Journal of Research and Development*, vol. 46, pp. 169–180, Mar. 2002.

[34] (2008, Apr.) The EPFL-EKV MOSFET model equations for simulation, version 2.6, rev. ii. [Online]. Available: http://legwww.epfl.ch/ekv/pdf/ekv_v262.pdf

[35] C. Svensson, "Low voltage technologies," in *Low Power Design in Submicron Electronics*, W. Nebel and J. Mermet, Eds. Kluwer Academic Publishers, 1997.

[36] B. H. Calhoun, A. Wang, and A. Chandrakasan, "Device sizing for minimum energy operation in subthreshold circuits," in *Proc. of IEEE Custom Integrated Circuits Conference (CICC'04)*, Orlando, Fla, USA, Oct. 2004, pp. 95–98.

[37] D. Johns and K. Martin, *Analog Integrated Circuit Design*. Hoboken, NJ: John Wiley & Sons, Inc., 1997.

[38] A. Bryant, J. Brown, P. Cottrell, M. Ketchen, J. Ellis-Monaghan, and E. J. Nowak, "Low-power CMOS at vdd=4kt/q," in *Proc. of IEEE Device Resarch Conference (DRC'01)*, Notre Dame, IN, USA, June 2001, pp. 22–23.

[39] S. T. Oskuii, "Comparative study on low-power high-performance flip-flops," Master's thesis, Linköping University, Linköping, Sweeden, Dec. 2003.

[40] J. Millman and A. Grabel, *Microelectronics*. Singapore: McGraw-Hill Book Co., 1987.

[41] R. Gonzalez and M. Horowitz, "Energy dissipation in general purpose microprocessors," *IEEE Journal of Solid-State Circuits*, vol. 31, pp. 1277–1284, Sept. 1996.

[42] J. U. Horstmann, H. W. Eichel, and R. L. Coates, "Metastability behavior of CMOS ASIC flip-flops in theory and test," *IEEE Journal of Solid-State Circuits*, vol. 24, pp. 146–157, Feb. 1989.

[43] S. S. Wagstaff, *Cryptoanalysis of Number Theoretic Ciphers*. Boca Raton, Florida: CRC Press, 2002.

[44] C. de Cannière, A. Biryukov, and B. Preneel, "An introduction to block cipher cryptoanalysis," *Proceedings of the IEEE*, vol. 94, pp. 346–356, Feb. 2006.

[45] S. B. Örs, F. Gürkaynak, E. Oswald, and B. Preneel, "Power-analysis attack on an ASIC AES implementation," in *Proc. of IEEE International Conference on Information Technology: Coding and Computing (ITCC'04)*, vol. 2, Las Vegas, NE, USA, Apr. 2004, pp. 546–552.

[46] F.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.

[47] J. Park, H. Lee, and J. Ha, "A differential power analysis attack of block cipher based on the hamming weight of internal operation unit," vol. 2, Guangzhou, China, Nov. 2006, pp. 1375–1380.

[48] L. Batina, N. Mentens, and I. Verbauwhede, "Side-channel issues for designing secure hardware implementations," in *Proc. of IEEE International On-line Testing Symposium (IOLTS'05)*, Saint Raphael, France, July 2005, pp. 118–121.

[49] D. D. Hwang, P. Schaumont, K. Tiri, and I. Verbauwhede, "Securing embedded systems," *IEEE Security & Privacy*, pp. 40–49, June 2006.

[50] H. Bar-El. (2008, Apr.) Introduction to side channel attacks. White Paper from Discretix Technologies Ltd. [Online]. Available: http://www.discretix.com/wp.shtml

[51] P. Kocher, J. Jaffe, and B. Jun. (1998) Introduction to differential power analysis and related attacks. Draft document from Cryptography Resarch. [Online]. Available: http://www.fit.vutbr.cs/~cvrcek/cards/dpa/index1.htm.en

[52] G. F. Bouesse, M. Renaudin, A. Witon, and F. Germain, "A clockless low-voltage AES crypto-processor," in *Proc. of IEEE European Solid State Circuit Conference (ESSCIRC'05)*, Grenoble, France, Sept. 2005, pp. 403–406.

[53] (2008, Apr.) CSRC - cryptographic toolkit, AES archive. [Online]. Available: http://csrc.nist.gov/archive/aes/

[54] D. Shang, F. Burns, A. Bystrov, A. Koelmans, D. Sokolov, and A. Yakovlev, "A low and balanced power implementation of the AES security mechanism using self-timed circuits," in *Proc. of IEEE Power and Timing Modeling, Optimization and Simulation Workshop (PATMOS'04)*, ser. Lecture Notes in Computer Science, vol. 3254. Springer, 2004, pp. 471–480.

[55] N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, "A systematic evaluation of compact hardware implementations for the Rijndael S-Box," in *Proc. of Cryptographers' Track RSA Conference (CT-RSA'05)*, ser.

Lecture Notes in Computer Science, vol. 3376. Springer, 2005, pp. 323–333.

[56] (2001, Nov.) FIPS 197: Advanced Encryption Standard. National Institute of Standards and Technology. [Online]. Available: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[57] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES SBoxes," in *Proc. of Cryptographers' Track RSA Conference (CT-RSA'02)*, ser. Lecture Notes in Computer Science, vol. 2271. Springer, 2002, pp. 67–78.

[58] H. Brunner, A. Curiger, and M. Hofstetter, "On computing multiplicative inverses in GF(2^m)," *IEEE Transactions on Computers*, vol. 42, pp. 1010–1015, Aug. 1993.

[59] J. Bierbrauer, *Introduction to coding theory*. Boca Raton, FL: Chapman & Hall/CRC, 2004.

[60] T. Good and M. Benaissa, "Pipelined AES on FPGA with support for feedback modes (in a multi-channel environment)," *IET Information Security*, vol. 1, pp. 1–10, Mar. 2007.

[61] V. Rijmen. (2008, Apr.) Efficient implementation of the Rijndael S-box. [Online]. Available: http://www.iaik.tugraz.at/Research/ ... krypto/AES/old/řijmen/rijndael/sbox.pdf.

[62] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-Box optimization," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security Advances in Cryptology (ASIACRYPT'01)*, ser. Lecture Notes in Computer Science, vol. 2248. Springer, 2001, pp. 239–254.

[63] H. P. Alstad and S. Aunet, "Seven subthreshold flip-flops cells," in *Proc. IEEE Norchip Conference (NORCHIP'07)*, Ålborg, Denmark, Nov. 2007, pp. 1–4.

[64] A. Chavan, G. Dukle, B. Graniello, and E. MacDonald, "Robust ultra-low power subthreshold logic flip-flop design for reconfigurable architectures," in *Proc. of IEEE International Conference on Reconfigurable Computing and FPGA's (ICRC'06)*, 2006, pp. 1–7.

[65] M. Horowitz, T. Indermaur, and R. Gonzalez, "Low-power digital design," in *Proc. of IEEE Symposium on Low Power Electronics*, Oct. 1994, pp. 8–11.

[66] T. Sundström and A. Alvandpour, "A comparative analysis of logic styles for secure IC's against DPA attacks," in *Proc. of IEEE Norchip Conference (NORCHIP'05)*, Nov. 2005, pp. 297–300.

[67] D. Canright, "A very compact s-box for AES," in *Workshop on Cryptographic Hardware and Embedded Systems (CHES'05)*, ser. Lecture Notes in Computer Science, vol. 3659. Washington DC, USA: Springer, Aug. 2005, pp. 441–455.

[68] S. Aunet and H. K. O. Berge, "Statistical simulations for exploring defect tolerance and power consumption for 4 subthreshold 1-bit addition circuits," *Computational and Ambient Intelligence*, vol. 4507, pp. 455–462, 2007.

BIBLIOGRAPHY

Paper I

Seven Subthreshold Flip-Flop Cells

25th IEEE Norchip 2007 Conference, Ålborg, Denmark, pp. 1-4, November 19th - 20th 2007

Seven Subthreshold Flip-Flop Cells

Håvard Pedersen Alstad
Department of Informatics
University of Oslo
Postbox 1080 Blindern
0316 Oslo, Norway
Email: haavarpa@ifi.uio.no

Snorre Aunet
Department of Informatics
University of Oslo
Postbox 1080 Blindern
0316 Oslo, Norway
Email: aunet@ieee.org

***Abstract*— For ultra-low-power applications, operating the transistors in their subthreshold region is an effective way of reducing the power dissipation of a circuit. This paper presents a comparative study of the performance of seven D-flip-flop cells operating in the subthreshold region, based on simulations in a 90 nm CMOS technology. Simulations have been performed with a supply voltage ranging from 150 mV to 350 mV. The best PDP and EDP numbers at 175 mV is 13 aJ and 10 yJs, respectively.**

I. Introduction

Flip-flops plays an important role in the power dissipation of modern synchronous digital circuits. Several methods for reducing the power dissipation of flip-flops have been proposed. Among the most promising methods, reducing the power supply voltage reduces the power dissipation dramatically [1]. This method has been known for decades [2], but has received more attention with the increasing demand for power-efficient electronics in recent years.

When the supply voltage is decreased below the threshold voltage of a transistor, the transistor is said to operate in its subthreshold region. Subthreshold operation is considered to be the most energy-efficient solution for low-power applications where performance is of secondary importance [3], [4].

II. Energy Consumption in CMOS

The total power dissipation of a circuit can be expressed as the sum of the static and the dynamic power dissipation component [5]. In traditional CMOS circuitry operating with a power supply voltage significant above the transistors threshold voltage, the dynamic power dissipated while charging and discharging of the circuit capacitance during transistor switching has been the dominant power dissipation component.

The dynamic power dissipation can be approximated with [6]:

$$P_{\mathrm{dyn}} = \frac{1}{2} \cdot \alpha \cdot C_{\mathrm{L}} \cdot V_{\mathrm{DD}}^2 \cdot f \tag{1}$$

where α is the probability of a signal transition within a clock period, C_{L} is the circuit capacitance to switch, V_{DD} is the power supply voltage and f is the clock frequency.

From this equation, it can be observed that the dynamic power dissipation depends quadratically on the power supply voltage, hence reducing V_{DD} is an effective way to reduce the dynamic power dissipation.

Static power dissipation occurs due to non-ideal secondary CMOS effects such as subthreshold leakage current and other leakage currents in the transistor. Assuming a constant leakage current, the static power dissipation is given as [5]:

$$P_{\mathrm{static}} = I_{\mathrm{static}} V_{\mathrm{DD}} \tag{2}$$

Subthreshold leakage current for $V_{\mathrm{gs}} < V_{\mathrm{tn}}$ for an n-type MOS transistor is given by [4] :

$$I_{\mathrm{ds}} = I_0 e^{(1-\kappa)V_{\mathrm{bs}}/V_T} e^{\kappa V_{\mathrm{gs}}/V_T} \left(1 - e^{-V_{\mathrm{ds}}/V_T} + V_{\mathrm{ds}}/V_0\right) \tag{3}$$

where V_{gs} is the gate-to-source voltage, V_{ds} is the drain-to-source voltage, V_{bs} is the substrate-to-source voltage (known as the body effect), I_0 is the zero-bias current for the given device, V_T is the temperature voltage, $V_T = kT/q$, V_0 is the Early voltage, and κ is the effectiveness of the gate potential in controlling the channel current.

By reducing the supply voltage, and thus also V_{gs}, below the threshold voltage, the transistor channel is never fully inverted, but operates in weak or moderate inversion when the transistor is in its 'on' state. For a n-type MOS transistor, weak inversion occurs when V_{gs} is approximately 100 mV or more below the threshold voltage V_{tn}, and strong inversion occurs when V_{gs} is 100 mV or more above V_{tn}. The region between weak and strong inversion is called moderate inversion [7].

III. Flip-Flops

An optimal flip-flop has low power dissipation, imposes no delay and gives a valid output at all time. In practical implementation, trade-offs between these parameters must be done.

Among significant parameters for characterizing a flip-flop's operation is its speed. Finding the maximum operating frequency of a flip-flop can be achieved by measuring the total delay required for a valid output is available after the input has been stabilized [8].

The delay of a flip-flop can be expressed as the time taken from the input changes to the output has stabilized. This delay can be expressed as $t_{\mathrm{delay}} = t_{\mathrm{setup}} + t_{\mathrm{ctq}}$, where t_{setup} is the time taken for the input to stabilize in the flip-flop and t_{ctq} is the time taken from the clock goes high to a valid output Q is available. From this conclusion, we get the following equation for the maximum delay of a flip-flop:

$$t_{\mathrm{delay}} = \max\left(\left(t_{\mathrm{setup}} + t_{\mathrm{ctq}}\right)_{,\mathrm{HL}}, \left(t_{\mathrm{setup}} + t_{\mathrm{ctq}}\right)_{,\mathrm{LH}}\right) \tag{4}$$

1-4244-1517-9/07/$25.00 (C)2007 IEEE

where HL is high-to-low transition.

Another important parameter is the power dissipation. The dynamic power dissipation of a flip-flop is data-pattern dependent and is directly proportional to the switching activity α [6]. The maximum power dissipation is reflected by applying a sequence 010101... (α = 1), while the minimum power dissipation is reflected by applying a constant high or low input signal (α = 0).

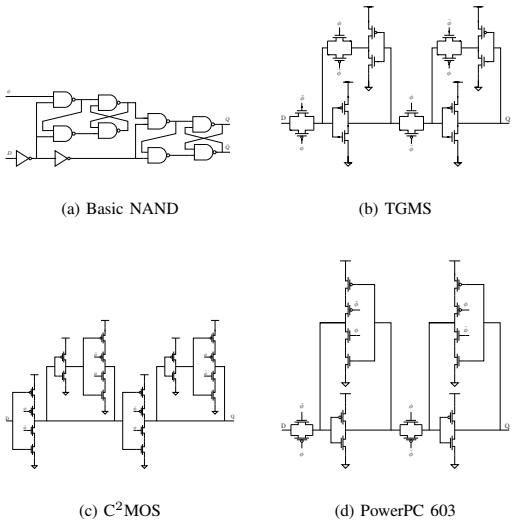
For this characterization of flip-flop cells performance in subthreshold operation, seven widely used and/or referred flip-flop cells have been selected. The selection has been based on the results from [9]. See Fig. 1 and 2 for schematic layout of cells. Sizing of transistors have been presented in Table I for all flip-flop cells except the *TSPC flip-flop*, which the transistors width in μm have been included in the schematic in Fig. 2(a) instead for clarifying reasons. For the *PowerPC 603 flip-flop*, a transistor width of W_p = 0.24 μm has been used for the feed-back C^2MOS transistors, while W_p = 0.36 μm has been used for all other p-type MOS transistors.

1) *Basic NAND flip-flop:* The basic NAND flip-flop is constructed out of NAND-gates. Each NAND-based latch require 16 transistors.
2) *Transmission-gate Master-Slave flip-flop:* The TGMS flip-flop is composed of two transmission gate based latches operating on complementary clocks. This flip-flop may be sensitive to clock-skew of it's two complementary clock-phases.
3) *C^{2}MOS flip-flop*: Build on the C^{2}MOS-logic style [10]. This flip-flop is in contrary to the TGMS insensitive of overlapping clocks.
4) *PowerPC 603:* This flip-flop is a combination of the TGMS and C^{2}MOS flip-flops, using clocked inverters instead of feedback transmission gates. It was used in the PowerPC 603 microprocessor data-path [11].

Three dynamic flip-flop-cells have also been tested. Dynamic flip-flop-cells use less transistors compared to their static counterparts, but suffers from only being able to drive a limited load and having a minimum operating frequency because of charge leakage on dynamic nodes due to subthreshold, gate and junction leakage.

5) *True Single-Phase Clock flip-flop:* The TSPC flip-flop require only one clock signal, and not its complementary [12]. This flip-flop produces a momentary glitch on the output when the input is low, regardless of the previous state of the output [5]. Transistor dimensioning shown in Fig. 2(a) is based on the results of [9].
6) *Dynamic Transmission-gate Master-Slave:* This flip-flop is built from a pair of back-to-back dynamic latches. As well as the static TGMS, the dynamic TGMS malfunctions if the clocks overlaps.
7) *Dynamic C^{2}MOS flip-flop*: A dynamic version of the C^{2}MOS flip-flop. The feed-back element in the latches has been removed.

For flip-flop requiring two phased clock, the complementary clock is produced using an in-cell inverter.



(a) Basic NAND (b) TGMS

(c) C^{2}MOS (d) PowerPC 603

Fig. 1. Static flip-flop cells

TABLE I
TRANSISTOR SIZING

Flip-flop cell	W_n (μm)	L_n (μm)	W_p (μm)	L_p (μm)
Basic NAND	0.2	0.2	0.36	0.2
TGMS	0.24	0.2	0.36	0.2
C^{2}MOS	0.24	0.2	0.36	0.2
PowerPC 603	0.24	0.2	0.36 / 0.24	0.2
Dynamic TGMS	0.24	0.2	0.36	0.2
Dynamic C^{2}MOS	0.24	0.2	0.36	0.2

IV. RESULTS

The characterization of the flip-flop cells have been achieved by simulation on a 90 nm standard CMOS process with a threshold voltage of V_{tn} = 0.24 V and V_{tp} = -0.29 V.

All flip-flops are simulated with a power supply voltage ranging from 350 mV down to 150 mV at an operating frequency of 1 MHz. For power dissipation analysis, a maximum power dissipation pattern α = 1 and no external load was applied. For verifying operability and delay characterization the test bench setup in Fig. 2(d) has been used, and the input waveform from Fig. 3(a) was applied.

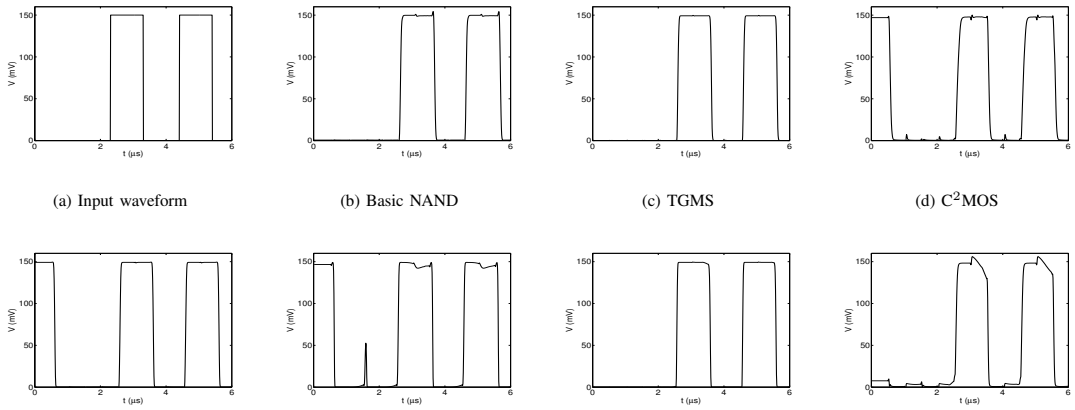
Figure 4 shows the simulation result for all seven circuits, regarding delay t_{delay}, power dissipation, power-delay product (PDP) and energy-delay product (EDP), with respect to V_{DD}.

Table II presents the figures for V_{DD} = 150 mV.

V. DISCUSSION

The simulation result of the *basic NAND flip-flop* shows a delay time of 284 ns and a power dissipation of 717 pW. Increasing the power supply voltage to approximately the threshold voltage, V_{DD} = 250 mV, the delay time decreases to

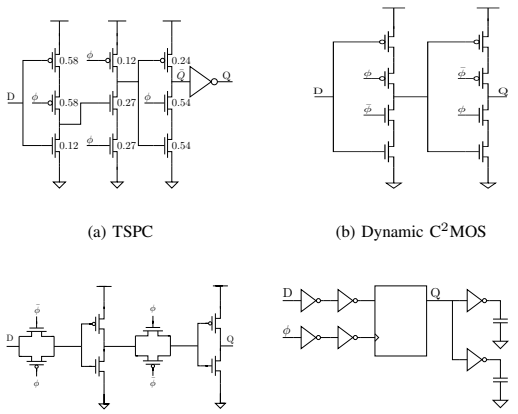
1-4244-1517-9/07/$25.00 (C)2007 IEEE



(a) Input waveform (b) Basic NAND (c) TGMS (d) C^{2}MOS

(e) PowerPC 603 (f) TSPC (g) Dynamic TGMS (h) Dynamic C^{2}MOS

Fig. 3. Example waveforms



(a) TSPC (b) Dynamic C^{2}MOS

(c) Dynamic TGMS (d) Simulation test bench

Fig. 2. Dynamic flip-flop cells and test bench

TABLE II
FLIP-FLOP METRICS, V_{DD} = 150 MV

Flip-flop cell	Delay [ns]	Power [pW]	PDP [aJ]	EDP [yJs]
Basic NAND	284.2	716.6	203.7	578.9
TGMS	129.8	332.7	43.2	56.0
C^{2}MOS	129.6	350.6	45.4	58.8
PowerPC 603	119.7	284.9	34.1	40.8
TSPC	121.2	279.0	33.8	41.0
Dyn. TGMS	83.7	199.4	16.7	14.0
Dyn. C^{2}MOS	77.9	165.5	12.9	10.0

38 ns while the power dissipation increases to 1.7 nW. These results are the worst overall results in this simulation.

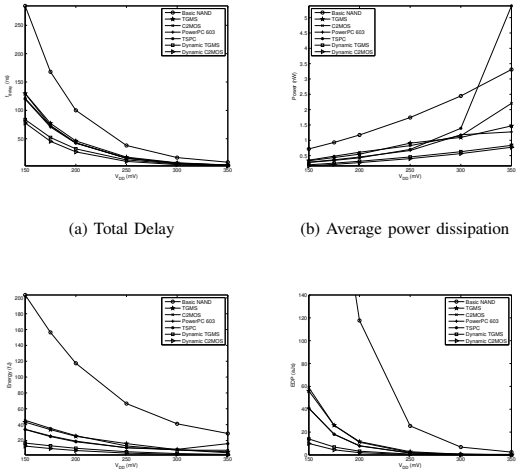
The *dynamic TGMS* and the *dynamic C^{2}MOS* shows the best performance on all figures regarding delay and power dissipation, with the C^{2}MOS version slightly better than the TGMS. At 250 mV, the delay time and power dissipation of the dynamic TGMS and dynamic C^{2}MOS are 12.7 ns/ 455 pW and 10.1 ns/ 402 pW, respectively. But as shown in Fig. 3(h), the output signal of the dynamic C^{2}MOS with the load of two inverters gets significantly degraded as the power supply voltage is lowered below the threshold limit.

For driving a high load, the static *PowerPC 603 flip-flop* shows the best overall performance, with a delay time of 16 ns and a power dissipation of 666 pW at 250 mV. If the flip-flop is driving a lower load, the dynamic TGMS cell offers less delay and power dissipation, providing 20% lower delay time and 30% lower power dissipation compared to the PowerPC 603 flip-flop at V_{DD} 250 mV. Dynamic flip-flops lack the ability are not able to hold the output signal for a long period of time, and should not be used in combination with power saving techniques such as idle and sleep mode.

Analysis of the *TSPC flip-flop* shows that it provides a medium delay compared to the other flip-flops tested. From the transient analysis in Fig. 3(f), the effect of a glitch on the output when D is low for following periods can clearly be seen in the second period. While increasing the power supply voltage to 300 mV, it shows a power dissipation in the middle of the other test results. But as the power supply voltage is being increased to 350 mV, the power dissipation increases almost by a factor of 3 with 50 mV increase in V_{DD}.

When the flip-flops are operated in the subthreshold region, the power dissipation P_{total} is dominated by the static power dissipation component P_{static}. Because of this, the power dissipation increases approximately linear with increasing V_{DD}

1-4244-1517-9/07/$25.00 (C)2007 IEEE



(a) Total Delay

(b) Average power dissipation

(c) Power Delay Product

(d) Energy Delay Product

Fig. 4. Simulation results

(2), as shown in Fig. 4(b). The power dissipation increases faster as the transistors are operated in stronger inversion. This effect is especially seen for the *TSPC flip-flop*, where the average power dissipation increases with a factor 1 when V_{DD} is increased from 250 mV to 300 mV and a factor 2.9 when V_{DD} is increased by another 50 mV to 350 mV.

Both the *PDP* and *EDP* results in Fig. 4(c) and 4(d) show a reduction in figures as the power supply voltage is increased. Looking at the time delay and power dissipation development in Fig. 4(a) and 4(b), it is seen that the delay time decreases faster that the power dissipation increases. This observation indicates that flip-flops may not benefit from being operated in the subthreshold region for applications where operation speed is of a concern. Work done on characterization of combinational logic in the subthreshold region [13], shows that the PDP decreases while lowering the supply voltage for this logic type. This would indicate that complete IC systems with a combination of combinational and sequential logic may benefit of operating in the subthreshold region with regards to the PDP metrics.

Studies done in [14] on a FFT-processor indicates that the best delay vs. energy dissipation relationship occurs when the transistors are operated with a power supply voltage between 350 mV and 400 mV for that particular case.

VI. Conclusion

This paper has examined subthreshold performance of seven commonly used flip-flop-cells. A power dissipation as low as 165.5 pW has been achieved at a supply voltage of 150 mV. Low power dissipation is important in some low-power application, and lowering the supply voltage is the most effective way of decreasing the power dissipation. This comes at the cost of the performance.

Based on the simulation results, it is shown that dynamic flip-flops such as the dynamic TGMS and the dynamic C^2MOS shows both the lowest delay and average power dissipation when the switching activity factor α is high. By operating in the subthreshold region, the subthreshold leakage effect that degrades the maximum holding time of dynamic cells is reduced, it is achieved to reduce discharging of dynamic nodes, which may effect the reliability of dynamic cells if its not taken into account when designing the circuit.

If a static flip-flop topology is desired, the PowerPC 603 flip-flop cell offers both the best delay time and power dissipation for this design topology with a delay time of 120 ns and a power dissipation of 285 pW at V_{DD} = 150 mV.

For practical implementation on a circuit with combinational logic, a supply voltage as low as 150 mV may not be possible to achieve because of process variations [15], [16].

All simulations have been performed on typical process corners at room temperature. For a more extensive analysis of the flip-flop cells with respect of minimum operation voltage and performance, simulation with different transistor dimensioning on layout at different process corners and with respect to temperature variations, as well as statistical mismatch would be instructive [16].

References

[1] Rabaey, J., Pedram, M., Landman, P.: Low Power Design Methodologies. Kluwer Academic Publishers, Boston (1995)
[2] Swanson, R.M., Meindl, J.D.: Ion-implanted complementary MOS transistors in low-voltage circuits. IEEE J. S.-S. C. **7** (1972) 146–153
[3] Soeleman, H., Roy, K., Paul, B.C.: Robust subthreshold logic for ultra-low power operation. IEEE Tran. on VLSI Systems **9** (2001) 90–99
[4] Andreou, A.G., et al.: Current-mode subthreshold MOS circuits for analog VLSI neural systems. IEEE T. Neural Netw. **2** (1991) 205–213
[5] Weste, N.H.E., Harris, D.: CMOS VLSI Design - A Circuits and Systems Perspective. Addison-Wesley, Boston, MA (2005)
[6] Xue, S., Oelmann, B.: Comparative study of low-voltage performance of standard-cell flip-flops. Proc. of IEEE ICECS 2001 **2** (2001) 953–957
[7] Johns, D., Martin, K.: Analog Integrated Circuit Design. John Wiley & Sons, Inc., Hoboken, NJ (1997)
[8] Unger, S.H., Tan, C.J.: Clocking schemes for high-speed digital systems. IEEE Trans. Comput. **C-35** (1986) 880–895
[9] Oskuii, S.T.: Comparative study on low-power high-performance flip-flops. Master's thesis, Linkoping University (2003)
[10] Suzuki, Y., Odagawa, K., Abe, T.: Clocked CMOS calculator circuitry. IEEE J. Solid-State Circuits **SC-8** (1973) 462–469
[11] Gerosa, G., et al.: A 2.2 W, 80 MHz superscalar RISC microprocessor. IEEE J. Solid-State Circuits **29** (1994) 1440–1452
[12] Yuan, J.R., Karlsson, I., Svensson, C.: A true single-phase-clock dynamic CMOS circuit technique. IEEE J. S.-S. C. **SC-22** (87) 899–901
[13] Granhaug, K., Aunet, S.: Six subthreshold full adder cells characterized in 90 nm CMOS technology. In: 2006 IEEE Design and Diagnostics of Electronic Circuits and system. (2006) 27–32
[14] Wang, A., Chandrakasan, A.: A 180 mV subthreshold FFT processor using a minimum energy design methodology. IEEE J. Solid-State Circuits **40** (2005) 310–319
[15] Granhaug, K., Aunet, S.: Improving yield and defect tolerance in multifunction subthreshold CMOS gates. In: Defect and Fault-Tolerance in VLSI Systems. 21st IEEE International Symposium on. (2006) 20–28
[16] Calhoun, B.H., Wang, A., Chandrakasan, A.: Modeling and sizing for minimum energy operation in subthreshold circuits. IEEE J. Solid-State Circuits **40** (2005) 1778–1786

1-4244-1517-9/07/$25.00 (C)2007 IEEE

Paper II

Three Subthreshold Flip-Flop Cells Characterized in 65 nm and 90 nm CMOS Technology

11th IEEE Workshop on Design and Diagnostics of Electronic Systems, pp. 8-11, Bratislava, Slovakia, April 16-18, 2008

Three Subthreshold Flip-Flop Cells Characterized in 90 nm and 65 nm CMOS Technology

Håvard Pedersen Alstad
Dept. of Informatics, University of Oslo
P.b. 1080 Blindern, 0316 Oslo, Norway
Email: haavarpa@ifi.uio.no

Snorre Aunet
Dept. of Informatics, University of Oslo
P.b. 1080 Blindern, 0316 Oslo, Norway
Email: aunet@ieee.org

***Abstract*— This paper examines three different flip-flop designs in subthreshold operation. All flip-flops are simulated in a 65 nm and 90 nm process with a supply voltage ranging from 125 mV to 1 V. Process variations are examined at different process corners.**

Successful operations of a PowerPC 603 flip-flop at all process corners with a supply voltage down to 125 mV is shown at 65 nm. The best PDP and EDP numbers of flip-flops design at $V_{\rm DD}$ = 200 mV in this paper are 53.6 aJ and 0.88 yJs, respectively.

I. Introduction

Several methods for reducing the power consumption of flip-flops have been proposed. Among the most promising methods, reducing the power supply voltage offers the most direct and dramatic means of reducing the power consumption [1]. When the supply voltage $V_{\rm DD}$ is decreased below the absolute value of a transistors threshold voltage V_T, the transistor is said to operate in its subthreshold region. Presently, subthreshold operation is considered to be the most energy-efficient solution for low-power applications where performance is of secondary importance [2], [3]. This method has been known for decades [4], but has in recent years received more attention with the increasing demand for power-efficient electronics. Applications well suitable for subthreshold operations include wearable medical equipment such as hearing aids and pacemakers, wrist-watch computers, self-powered devices and wireless sensor networks [2], [5], [6].

Three flip-flop designs, based on results from [7] and [8], have been chosen for characterization in this work. These flip-flops are characterized operating with a power supply voltage ranging from deep subthreshold operation at $V_{\rm DD}$ = 125 mV to nominal superthreshold for the processes being used, $V_{\rm DD}$ = 1 V. A brief introduction to energy consumption nature of CMOS is given in Sec. II. In Sec. III a presentation of selected flip-flop designs is given. Simulation results including delay timing, power consumption, Power-Delay Product and Energy-Delay Product, as well as process corners characterizations are presented in Sec. IV and discussed in Sec. V. Summary and conclusion are given in Sec. VI.

II. Energy Consumption in CMOS

The total power dissipation of a circuit can be expressed as the sum of the static and the dynamic power dissipation components [9]. The dynamic power has been the dominant power dissipation component in traditional CMOS, operating with a power supply voltage significant above the transistors threshold voltage.

The dynamic power dissipation, dissipated while charging and discharging the circuit capacitance during transistor switching, can be approximated to [10]:

$$P_{\rm dynamic} = \frac{1}{2} \cdot \alpha \cdot C_{\rm L} \cdot V_{\rm DD}^2 \cdot f \quad (1)$$

where α is the probability of a signal transition within a clock period, $C_{\rm L}$ is the circuit capacitance to switch, $V_{\rm DD}$ is the power supply voltage and f is the clock frequency. The dynamic power dissipation depends quadratically on the power supply voltage, hence reducing $V_{\rm DD}$ is an effective way to reduce the dynamic power dissipation.

Static power dissipation occurs due to non-ideal secondary CMOS effects such as subthreshold leakage current and other leakage currents in the transistor. Assuming a constant leakage current, the static power dissipation is given as the product of the leakage current and $V_{\rm DD}$ [9]. Subthreshold leakage current for $V_{\rm gs} < V_{\rm Tn}$ for an n-type MOS transistor is given by [3] :

$$I_{\rm ds} = I_0 e^{(1-\kappa)V_{\rm bs}/V_t} e^{\kappa V_{\rm gs}/V_t} \left(1 - e^{-V_{\rm ds}/V_t} + V_{\rm ds}/V_0\right) \quad (2)$$

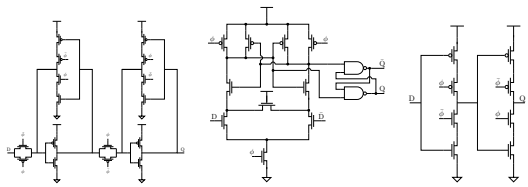
where $V_{\rm gs}$ is the gate-to-source voltage, $V_{\rm ds}$ is the drain-to-source voltage, $V_{\rm bs}$ is the substrate-to-source voltage (known as the body effect), I_0 is the zero-bias current for the given device, V_t is the temperature voltage, $V_t = kT/q$, V_0 is the Early voltage, and κ is the effectiveness of the gate potential in controlling the channel current.

By reducing the power supply voltage with 100 mV in subthreshold operation, the on-current I_{on} is reduced with a factor of 10 [6]. Such reduction leads to huge reduction in power consumption.

III. Flip-Flops

Three widely used flip-flop designs have been selected for testing, based on the most promising candidates from simulations done in [7] and [8]. Fig. 1 shows schematic drawings of the designs. The *PowerPC 603* is a master-slave flip-flop using transmission gate latches with C^{2}MOS-based logic [11] in feed-back elements [12]. The *Sense-Amplifier based flip-flop* (SAFF) [13] consists of a sense-amplifier and a S-R latch capturing the output of the sense-amplifier. SAFF flip-flop was reported to work at the lowest $V_{\rm DD}$ in comparison

978-1-4244-2277-7/08/$25.00 ©2008 IEEE



(a) PowerPC 603 (b) SAFF (c) Dynamic C^{2}MOS

Fig. 1. Flip-flop designs and test bench setup

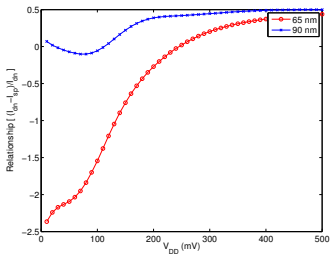


Fig. 2. Ratio between nMOS and pMOS currents in 65 nm and 90 nm process, $W_n = W_p$ and $L_n = L_p$

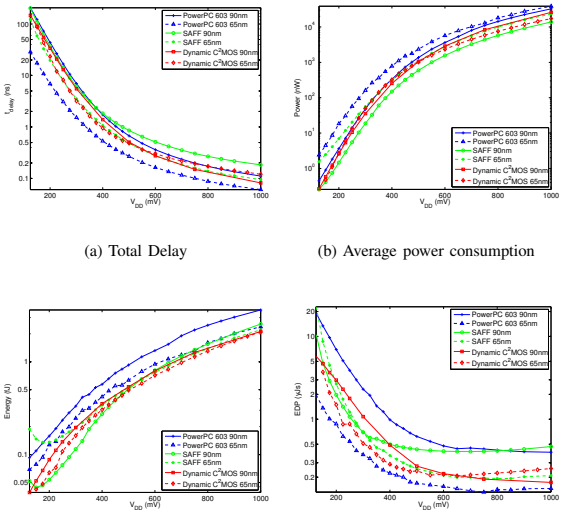
to other flip-flops tested in [10]. In the same work, SAFF also showed the best overall performance. *Dynamic C^{2}MOS* is a dynamic master-slave flip-flop built on the C^{2}MOS logic style, where the feed-back elements are removed. An inverter has been added for producing a two phased clock for the *PowerPC 603* and *dynamic C^{2}MOS* flip-flops.

Sizing of flip-flops operating in the subthreshold region should be done with other p/n-ratio than normal superthreshold CMOS. For minimum V_{DD} operation, the same current should go through the pMOS and nMOS transistor at the switching point [14], [15]. As shown in Fig. 2 it can be observed how the conductivity of an nMOS and pMOS transistor behave in respect to V_{DD}. For the test setup, $V_{\mathrm{gs-high}} = V_{\mathrm{DD}}$ has been used. For the 65 nm general purpose process used under the simulation, it is clearly shown how the transistor sizing must be changed for optimal sizing with respect of the supply voltage. Sizing used in this work is listed in Tab. I. For this paper, a relationship of $W_p = 0.67W_n$ has been chosen for this process. From the result in Fig. 2 it is indicated that this will give the best result at approximately $V_{\mathrm{DD}} = 150$ mV.

Running with a supply voltage of 150 mV at room temperature is well above the theoretical lower limit, reported to be in the range from 36 mV to 80 mV in current technologies by [16]. In the same work, it is stated that 100 mV can prove to be a practical lower limit for implementations. Some sort of more advanced logic than only inverters must be able to function, i.e. NAND and NOR gates. The lower limit at 36 mV is not likely to be reached by any technology according to [17].

TABLE I
TRANSISTOR SIZING

Flip-flop cell	W_{n} (μm)	L_{n} (μm)	W_{p} (μm)	L_{p} (μm)
PowerPC 65 nm	0.18	0.6	0.12	0.6
SAFF 65 nm	0.12	0.6	0.36	0.6
Dyn. C^{2}MOS 65 nm	0.24	0.12	0.12	0.12
PowerPC 90 nm	0.12	0.1	0.36	0.1
SAFF 90 nm	0.12	0.1	0.12	0.1
Dyn. C^{2}MOS 90 nm	0.12	0.1	0.36	0.1



(a) Total Delay (b) Average power consumption

(c) Power Delay Product (d) Energy Delay Product

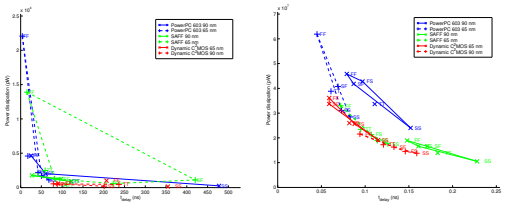
Fig. 3. Simulation results

IV. SIMULATION RESULTS

Flip-flop design characterization is achieved by simulation in general purpose 90 nm and 65 nm processes available from STMicroelectronics. For the 90 nm process, threshold voltages are given as V_{Tn} = 0.24 V and V_{Tp} = -0.29 V, while the 65 nm process has $V_{\mathrm{Tn}} \sim$ 0.21 V and $V_{\mathrm{Tp}} \sim$ -0.17 V. Flip-flops are simulated with V_{DD} ranging from 125 mV to 1 V.

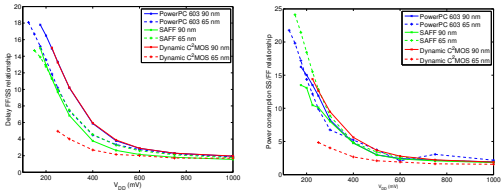
The test-bench setup from [7] has been used. Timing delay simulations have been simulated at a constant clock frequency of 1 MHz, while power consumption are calculated with simulations at maximum frequency, $\frac{1}{f} = t_{\mathrm{delay}}$. A maximum power consumption pattern $\alpha = 1$ is applied.

Simulation results for all flip-flop designs in the 90 nm and 65 nm process are shown in Fig. 3, regarding delay t_{delay}, power consumption, Power-Delay Product (PDP) and Energy-Delay Product (EDP), with respect to V_{DD}. The *dynamic C^{2}MOS* design was unable to operate correctly at 65 nm with minimum sized gates. With an increased gate length, as listed in Tab. I, this design was able to operate correctly.



(a) Corners at 150 mV (b) Corners at 1000 mV

Fig. 4. Corners at different supply voltages



(a) Delay (b) Power

Fig. 5. Ratio between FF and SS corner performance

In general, flip-flops in the 65 nm process show a lower delay time at the cost of higher power consumption compared to the same flip-flop designs in the 90 nm process. For subthreshold operations, the *PowerPC 603* has an increase in the EDP value of 10 times in the 90 nm process compared to the 65 nm process, while the *SAFF* shows a higher EDP value in 65 nm at low power supply voltages.

At 65 nm, *PowerPC 603* provides better delay and EDP figures than *SAFF* and *dynamic C²MOS*. *Dynamic C²MOS* has the lowest power consumption and PDP figures at subthreshold power supply voltages. At 90 nm, *dynamic C²MOS* has the lowest delay time, while *SAFF* has the best power and PDP results. In the supply voltage range between 175 mV and 400 mV, *SAFF* provides the best EDP, while *dynamic C²MOS* has lowest EDP figures at other values of V_{DD}.

Performance metrics at different process corners are shown in Fig. 4. This figure shows the delay time and corresponding power consumption at process corners. The lines are drawn to make it easier to differ one design from another. Corners failing during simulation (due to stuck-at-zero/ stuck-at-one or $t_{\mathrm{delay}} > 0.5t_{\mathrm{period}}$) are not drawn. A visualization of number of successful corners with respect to power supply voltage is shown in Fig IV. It is shown that the 65 nm process is able to work successful in all corners at the lowest V_{DD} for this test setup. *PowerPC603* operates successfully at 125 mV and *SAFF* at 150 mV in 65 nm, while both designs works successfully in all corners at 175 mV in 90 nm. The *dynamic C²MOS* requires at least $V_{\mathrm{DD}} = 225$ mV for ensuring successful operation in all corners in 90 nm.

The ratio between the FF and SS corners is shown in Fig. 5 with respect to V_{DD}. According to figures, the relative difference between corners are significantly higher in subthreshold.

Tab. II shows selected metrics in the TT corner at $V_{\mathrm{DD}} = 200$ mV. Lowest V_{DD} refers to the lowest simulated V_{DD} where the flip-flop successfully operates in all five corners.

V. Discussion

By reducing the supply voltage, power consumption of a single flip-flop may be reduced with as much as a factor of 20.000, according to Fig 3(b). This comes at the cost of increased delay time and thus lower maximum operating frequency. Many applications have power consumption

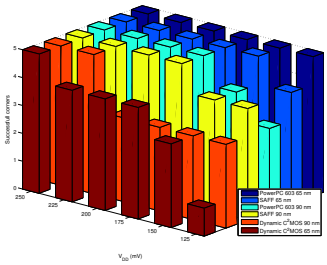


Fig. 6. Successful corners

management as primary concern and may have negligible timing requirements. Subthreshold CMOS may prove to be an excellent choice of technology for such applications.

As growing power-density emerge as a major challenge of todays and future CMOS technologies, due to circuits increased power density, efforts for decreasing the growing power-density trend must be done. In combination with massive parallelism and pipelining, it may be possible to maintain high performance and throughput while running in the subthreshold regime [16]. If so, performance of flip-flops may play a crucial part of the circuits overall performance.

According to simulation results, power consumption metric benefits most from subthreshold operation in comparison with the other metrics. In Fig. V, metrics of *PowerPC 603* at 65 nm for power supply voltage at 1 V and 125 mV are compared, and reduction factor with subthreshold operation is shown. As shown in the figure, PDP benefits from deep subthreshold operation in addition to power consumption. Timing and EDP metrics do not benefit from operating at this supply voltage in comparison with the other metrics. In Fig. V, metrics of *PowerPC 603* in 65 nm, running with power supply voltage of 1 V and 125 mV, are compared, and the increased performance when running in subthreshold operation compared to normal superthreshold operation is shown for each metric.

Transistor sizing must be done with target supply voltage in mind. Due to random doping fluctuations, the σ for V_T variation is proportional to $1/\sqrt{WL}$, so this will produce worst

TABLE II
FLIP-FLOP METRICS @ $V_{\mathrm{DD}} = 200$ MV, TT PROCESS CORNER

Cell name	t_{setup}	t_{hold}	t_{CCQ}	t_{delay}
PowerPC 603, 65 nm	2.7 ns	2.4 ns	4.3 ns	6.9 ns
SAFF, 65 nm	0.23 ns	17.5 ns	19.4 ns	19.6 ns
Dynamic C^{2}MOS, 65 nm	11.0 ns	1.2 ns	12.4 ns	23.3 ns
PowerPC 603, 90 nm	17.8 ns	24.3 ns	26.7 ns	44.3 ns
SAFF, 90 nm	1.5 ns	29.2 ns	35.7 ns	36.8 ns
Dynamic C^{2}MOS, 90 nm	19.0 ns	0.40 ns	14.8 ns	33.7 ns
Cell name	Power	PDP	EDP	V_{DDmin}
PowerPC 603, 65 nm	18.5 nW	127.6 aJ	0.88 yJs	125 mV
SAFF, 65 nm	6.9 nW	136.1 aJ	2.67 yJs	150 mV
Dynamic C^{2}MOS, 65 nm	2.7 nW	63.6 aJ	1.48 yJs	250 mV
PowerPC 603, 90 nm	3.3 nW	153.7 aJ	6.81 yJs	175 mV
SAFF, 90 nm	1.5 nW	53.6 aJ	1.97 yJs	175 mV
Dynamic C^{2}MOS, 90 nm	2.6 nW	88.1 aJ	2.97 yJs	225 mV

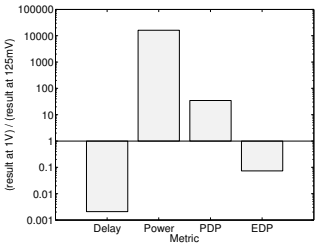


Fig. 7. Metrics improvement factor at $V_{\mathrm{DD}} = 125\,\mathrm{mV}$ vs. $V_{\mathrm{DD}} = 1\,\mathrm{V}$

case random V_T mismatch [18]. Mismatch of V_T leads to different current drive of nMOS and pMOS transistors, which may result in circuit failure. Body-bias regulations has been presented as a promising method for decreasing V_T variations [19]. V_T is stabilized by regulating the back-gate voltage of transistors with a small bias regulator circuit.

Simulations of the *dynamic C^{2}MOS* show some problems with running at low frequency. Due to its dynamic design, it lacks the ability to hold a signal for a longer period of time because of leakage currents. This makes this flip-flop design less ideal for use in subthreshold circuits with very low operating frequency or for designs with sleep mode ability. At 65 nm, this circuits requires 250 mV of supply voltage for running successfully in all corners.

Further simulations exploring performance at different temperatures would be instructive, as well would chip implementation for verification of simulations.

VI. CONCLUSION

According to the International Technology Roadmap for Semiconductors, power management is presently the primary issue across most CMOS application segments [20]. Dramatic measures must be taken to reduce the overall power consumption. Subthreshold operation is the most dramatic way to obtain reduction in power consumption.

Three different flip-flops has been tested for operation in the subthreshold region in a 90 nm and a 65 nm process at different process corners through simulations. As simulations indicates, flip-flops function well with V_{DD} scaled down in the subthreshold region. According to our simulations, *PowerPC 603* at 65 nm offers the best delay time, 28.7 ns, at $V_{\mathrm{DD}} =$ 125 mV. At the same supply voltage, *SAFF* at 90 nm offers the lowest power consumption, 256 pW, *dynamic C^{2}MOS* at 90 nm offers the best PDP figure, 39.1 aJ, and *PowerPC 603* at 65 nm offers the best EDP figure, 1.99 yJs.

Simulations indicate that flip-flops are able to operate at most process corners at very low supply voltages without malfunction. The test results indicate that the *PowerPC 603* static flip-flop cell would be best suitable for ultra-low-voltage operation, as it operates successful at all process corners at 125 mV in the 65 nm process.

REFERENCES

[1] J. Rabaey, M. Pedram, and P. Landman, *Low Power Design Methodologies*. Boston: Kluwer Academic Publishers, 1995.
[2] A. Wang and A. Chandrakasan, "A 180 mV subthreshold FFT processor using a minimum energy design methodology," *IEEE J. Solid-State Circuits*, vol. 40, pp. 310–319, Jan. 2005.
[3] A. G. Andreou *et al.*, "Current-mode subthreshold MOS circuits for analog VLSI neural systems," *IEEE T. Neural Netw.*, vol. 2, pp. 205–213, Mar. 1991.
[4] R. M. Swanson and J. D. Meindl, "Ion-implanted complementary MOS transistors in low-voltage circuits," *IEEE J. S.-S. C.*, vol. 7, pp. 146–153, Apr. 1972.
[5] H. Soeleman and K. Roy, "Ultra-low power digital subthreshold logic circuits," in *Proc. Low Power Electronics and Design*, 1999, pp. 94–96.
[6] L. Nazhandali *et al.*, "Energy optimization of subthreshold-voltage sensor network processors," in *Proc. Intl. Symp. on Computer Architecture*, 2005, pp. 197–207.
[7] H. P. Alstad and S. Aunet, "Seven subthreshold flip-flops cells," in *Proc. IEEE NorCHIP 2007*, Nov. 2007, pp. 1–4.
[8] B. Fu and P. Ampadu, "Comparative analysis of ultra-low voltage flip-flops for energy efficiency," in *Proc. IEEE ISCAS 2007*, pp. 1173–1176.
[9] N. H. E. Weste and D. Harris, *CMOS VLSI Design - A Circuits and Systems Perspective*. Boston, MA: Addison-Wesley, 2005.
[10] S. Xue and B. Oelmann, "Comparative study of low-voltage performance of standard-cell flip-flops," *Proc. of IEEE ICECS 2001*, pp. 953–957.
[11] Y. Suzuki *et al.*, "Clocked CMOS calculator circuitry," *IEEE J. Solid-State Circuits*, vol. SC-8, pp. 462–469, Dec. 1973.
[12] G. Gerosa *et al.*, "A 2.2 W, 80 MHz superscalar RISC microprocessor," *IEEE J. Solid-State Circuits*, vol. 29, pp. 1440–1452, Dec. 1994.
[13] M. Matsui *et al.*, "A 200 MHz 13 mm^2 2-D DCT macrocell using sense-amplifying pipeline flip-flop scheme," *IEEE J. Solid-State Circuits*, vol. 29, pp. 1482–1490, Dec. 1994.
[14] B. H. Calhoun, A. Wang, and A. Chandrakasan, "Device sizing for minimum energy operation in subthreshold circuits," *Proc. IEEE Custom Integrated Circuits Conference*, pp. 95–98, 2004.
[15] G. Schrom and S. Selberherr, "Ultra-low-power CMOS technologies," *International Semiconductor Conference*, pp. 237–246, 1996.
[16] E. J. Nowak, "Maintaining the benefits of CMOS scaling when scaling bogs down," *IBM J. Res. & Dev.*, vol. 46, pp. 169–180, Mar. 2002.
[17] C. Svensson, "Low voltage technologies," in *Low Power Design in Submicron Electronics*. Kluwer Academic Publishers, 1997.
[18] A. Chavan *et al.*, "Robust ultra-low power subthreshold logic flip-flop design for reconfigurable architectures," in *Proc. Reconfigurable Computing and FPGA's*, 2006, pp. 1–7.
[19] A. Bryant *et al.*, "Low-power CMOS at Vdd 4kt/q," in *Proc. Device Resarch Conference*, 2001, pp. 22–23.
[20] "International Technology Roadmap for Semiconductors, Executive Summary 2007," http://www.itrs.net/, Dec. 2007.

Paper III

Improving Circuit Security against Power Analysis Attacks with Subthreshold Operation

11th IEEE Workshop on Design and Diagnostics of Electronic Systems, pp. 12-13, Bratislava, Slovakia, April 16-18, 2008

Improving Circuit Security against Power Analysis Attacks with Subthreshold Operation

Håvard Pedersen Alstad
Dept. of Informatics, University of Oslo
P.B. 1080 Blindern, 0316 Oslo, Norway

Snorre Aunet
Dept. of Informatics, University of Oslo
P.B. 1080 Blindern, 0316 Oslo, Norway

***Abstract*— Countermeasures against side-channel attacks of cryptographic circuits have become of great concern when designing cryptographic and other sorts of circuits requiring secure handling of data. This paper suggests using subthreshold implementation for protection against power analysis attacks and presents a comparative analysis of a standard static CMOS 8-bit full adder cell, simulated in a 90 nm CMOS process, operating in the subthreshold and superthreshold region. A comparison of the correlation between input data and instantaneous power consumption is done. Circuit simulation and statistical analysis show that subthreshold operation gives orders of magnitude lower correlation between power consumption and data.**

I. Introduction

As cryptographic algorithms have become more secure against cryptoanalysis attack, several types of side channel attacks (SCA) on cryptographic IC have been reported (e.g. [1], [2]). Such attacks are physical attacks on the implementation of the circuit, exploiting physical measurable information emitted by the device, such as time delay and power consumption. With the increasing demand for secure data communication, it is becoming of greater importance to design with protection against side channel attacks in mind for certain applications. Differential Power Analysis (DPA) attack [2] is an effective SCA of great concern, based on statistical analysis of power consumption patterns.

Operating circuits with power supply voltage below the threshold voltage of transistors is a dramatic way to reduce the power dissipation [3], at the expense of operation speed. When the supply voltage V_{DD} is decreased below a transistors threshold voltage V_T, the transistor is said to operate in its subthreshold region. The I_{on}/I_{off} ratio can be reduced with as much as a factor of approximately 10^3 if V_{DD} is reduced from 1 V down to 150 mV. Research on subthreshold operation also indicates that the dynamic power consumption component is reduced, while the static power dissipation component is dominating the power dissipation. This can be used to make it harder to detect the switching activity, and therefore improve resistance against power analysis attack with subthreshold operation. Subthreshold implementations of large circuits have been proven to work in e.g. [4], [5].

It was shown in [6] how reduction of power supply voltage reduces the current profile of an AES crypto-processor. This paper intend to investigate the use of subthreshold supply voltage for protection against SCA. This work is inspired by the comparative analysis of logic styles done in [7] at normal supply voltages. A static CMOS 8-bit ripple carry adder is used for measuring the correlation between input data and instantaneous power consumption [8] at subthreshold operation with a power supply voltage, V_{DD}, of 200 mV and superthreshold operation at the nominal power supply voltage of the process being used, $V_{\mathrm{DD}} = 1$ V. In [9], the use of floating gate techniques in combination with subthreshold operation was presented as a method for increasing the resistance against SCA.

978-1-4244-2277-7/08/$25.00 ©2008 IEEE

II. Side-channel Attacks

When cryptography is used in computer systems, these ciphers are prone to attack on their physical implementation, denoted SCA. It was shown in [2] how a cryptographic cipher implemented in an electronic circuit produces timing information, power consumption variations due to switching activity and radiates electromagnetic traces that can easily be measured and abused for finding the secret key at a low cost.

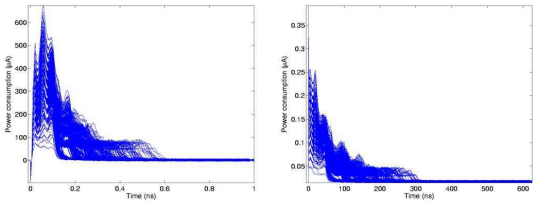
A power analysis type of SCA uses the variation in power consumption correlated to the operations done to calculate the secret key being used. An effective power analysis attack was presented in [2] and was named DPA. In [10], a successful attack on an actual cryptographic circuit implementation was presented. This implementation of the attack required only 4000 measurement to extract the right 8 MSB of the secret encryption key of a hardware implementation of the AES cryptographic algorithm.

Reducing the signal magnitude and the power dissipation are two methods proposed for reducing the side-channel information leaked through the chip. By reducing V_{DD} into the subthreshold region, exponential reduction in the power consumption is achieved.

III. Test Setup and Simulation Results

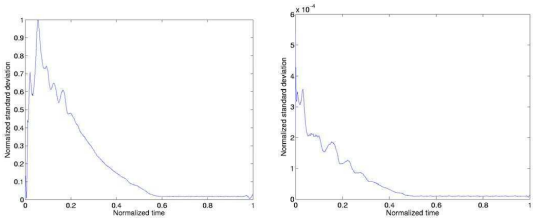
A circuit with instantaneous current uncorrelated to input signals is secure from SCA [8]. For measuring the resistance against power analysis attack, the correlation between the input vector and the corresponding current drawn from the power supply has been calculated.

The power consumption of the adder and the input drivers are taken into account, as well as the output loads [8]. A standard static CMOS full adder used for subthreshold operation in [11] is chosen as the building block for the 8-bit ripple adder. Transistor sizing from [11] is used in a 90 nm



(a) Current drawn, $V_{\mathrm{DD}} = 1\,\mathrm{V}$ (b) Current drawn, $V_{\mathrm{DD}} = 200\,\mathrm{mV}$

Fig. 1. Power consumption for 1000 random input combinations



(a) std, $I_{\mathrm{V_{DD}}}$@$V_{\mathrm{DD}} = 1\,\mathrm{V}$ (b) std, $I_{\mathrm{V_{DD}}}$@$V_{\mathrm{DD}} = 200\,\mathrm{mV}$

Fig. 2. Correlation between input values and power dissipation

1V CMOS process. For each power supply voltage simulated, 1000 random combinations of two 8-bit signals wasare applied as input signals, and the corresponding power consumption is measured as the current drawn from the power supply. The power consumption of the adder, the input drivers and the output loads are taken into account.

Fig. 1 shows the simulated power consumption as the instantaneous current drawn from the power supply in superthreshold and subthreshold operation for 1000 input combinations. Maximum current for $V_{\mathrm{DD}} = 1\,\mathrm{V}$ is $600\,\mu\mathrm{A}$, while the maximum current for $V_{\mathrm{DD}} = 200\,\mathrm{mV}$ is $0.41\,\mu\mathrm{A}$.

The standard deviation (std) of the current drawn from the power supply is shown in Fig 2. For making comparison of the different power supply voltage easier, the standard deviation is normalized [8]. At superthreshold operation, highest maximum normalized standard deviation, 1.0, occurs. The maximum normalized standard deviation when $V_{\mathrm{DD}} = 200\,\mathrm{mV}$ is 0.00052.

IV. Discussion

By reducing V_{DD} the supply voltage down into the subthreshold region, our simulation results shows that the correlation between input signal and power consumption, measured as current drawn from V_{DD}, is reduced with a factor of 1900, while the circuits calculation time is increased with a factor of approximately 600. As the signal magnitude is decreased, the signal-to-noise ratio increases, making the circuit more sensitive to noise.

Fig. 2 shows that the highest variance of the power consumption occurs at the start of calculation, when input data changes. After the initial calculation has been done, the carry starts to ripple through the adder. After the calculation is completed, the power consumption is negligible.

While a reduction in the correlation between the input signal and the power consumption is achieved, a complete protection against power analysis attacks is not attained while some degree of correlation exists. Subthreshold operation makes SCA harder to perform, but does not offer complete protection.

Further investigation on the reduction of signal magnitude by combining subthreshold operation with logic styles where power consumption has been reported to be less sensitive to switching activity (e.g. [7], [8], [12]) would be of high interest for making cryptographic circuits more resistant against SCA. Chip measurements would be helpful for verification.

V. Conclusion

In modern cryptosystems SCA emerge as a major security threat. Design of a cryptographic circuits must be done with minimization of side-channel information leakage in mind.

This paper has through simulations on a 8 bit full adder shown how subthreshold operation can reduce the correlation between data being processed and power dissipation measured as current drawn from the power supply voltage with a factor of 1900, at the cost of 600 times longer calculation time. As indicated by simulations, standard CMOS logic operated in the subthreshold region provides orders of magnitude improved security against power analysis attacks.

References

[1] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Proc. CRYPTO*, vol. LNCS 1109, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proc. CRYPTO*, vol. LNCS 1666, 1999, pp. 388–397.

[3] D. Liu and C. Svensson, "Trading speed for low power by choise of supply and threshold voltages," *IEEE J. Solid-State Circuits*, vol. 28, pp. 10–17, Jan. 1993.

[4] A. Wang and A. Chandrakasan, "A 180 mV subthreshold FFT processor using a minimum energy design methodology," *IEEE J. Solid-State Circuits*, vol. 40, pp. 310–319, Jan. 2005.

[5] S. Hanson *et al.*, "Performance and variability optimization strategies in a sub-200mV, 3.5pJ/inst 11nW subthreshold processor," *Symp. on VLSI Circuits*, pp. 152–153, 2007.

[6] G. F. Bouesse *et al.*, "A clock-less low-voltage AES crypto-processor," in *Proc. IEEE ESSCIRC*, 2005, pp. 403–406.

[7] K. Tiri and I. Verbauwhede, "Charge recycling sense amplifier based logic: securing low power security ICs against DPA [differential power analysis]," in *Proc. IEEE ESSCIRC*, 2004, pp. 179–182.

[8] T. Sundström and A. Alvandpour, "A comparative analysis of logic styles for secure IC's against DPA attacks," in *Proc. IEEE Norchip*, Nov. 2005, pp. 297–300.

[9] O. Mirmotahari and Y. Berg, "Proposal for a ultra low voltage NAND gate to withstand power analysis attacks," in *Proc. World Academy of Science, Engineering and Technology*, vol. 25, Nov. 2007, pp. 83–87.

[10] S. B. Örs *et al.*, "Power-analysis attack on an ASIC AES implementation," in *Proc. Information Technology: Coding and Computing*, vol. 2, 2004, pp. 546–552.

[11] S. Aunet and H. K. O. Berge, "Statistical simulations for exploring defect tolerance and power consumption for 4 subthreshold 1-bit addition circuits," in *Proc. IWANN*, vol. LNCS 4507, 2007, pp. 455–462.

[12] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. of Design Automation and Test in Europe Conference*, Feb. 2004, pp. 246–251.

Paper IV

Subthreshold AES S-box with Increased Power Analysis Resistance

Submitted for conference publication.

Subthreshold AES S-Box with Increased Power Analysis Resistance

Håvard Pedersen Alstad
Department of Informatics, University of Oslo
Postbox 1080 Blindern, 0316 Oslo, Norway
Email: haavarpa@ifi.uio.no

Snorre Aunet
Department of Informatics, University of Oslo
Postbox 1080 Blindern, 0316 Oslo, Norway
Email: aunet@ieee.org

***Abstract*— Operation in subthreshold region is tested for increasing resistance of the AES S-box against power analysis attacks. The non-linear S-box (Substitute Bytes) operation is one of the major building blocks of the AES algorithm. A compact 4 stage pipelined and asynchronous S-box is implemented in 90 nm CMOS technology. The S-box is simulated in normal superthreshold and subthreshold operation. The correlation and standard deviation of instantaneous power consumption is calculated. Our simulation results indicate orders of magnitude lower correlation between power consumption and processed data. The increased resistance against power analysis attacks comes at the cost of 340 times longer execution time. Our S-box has a throughput of 7.37 Mbit/s in subthreshold operation. The throughput is increased to 19.88 Mbit/s when introducing 4 pipeline stages.**

I. Introduction

Several types of side-channel attacks on cryptographic ICs have been reported lately [1]–[3]. Side-channel attacks are physical attacks on the implementation of the circuit exploiting physical measurable information emitted by the device, such as time delay and power consumption. Side-channel attacks have become a major threat to implementation of modern cryptographic ciphers immune against cryptoanalysis attacks. A cryptographic cipher implemented in an IC produces variation in power consumption and electromagnetic radiation due to switching activity of transistors. These variations are easily measurable with physical access to the IC, and may be used to extract internal information from the circuit. Differential Power Analysis (DPA) attack [2] is an effective side-channel attack of great concern, based on statistical analysis of power consumption patterns.

In [3], a successful DPA attack on an actual implementation was presented. The attacker extracted the correct 8 MSB of the secret encryption key in a hardware implementation of the AES cryptographic algorithm [4] by measuring the variance in power consumption when different input vectors were applied. A successful attack has reported power traces of 8000 encryptions as sufficient to extract the secret key of an unprotected AES implementation [5], [6]. The attacker required less than 3 minutes to extract the key. In comparison, 2^{128} tests are required to brute force the AES algorithm. It corresponds to an increase in attack time of $4.25 \cdot 10^{34}$ times compared to the number of tests required for a successful DPA attack.

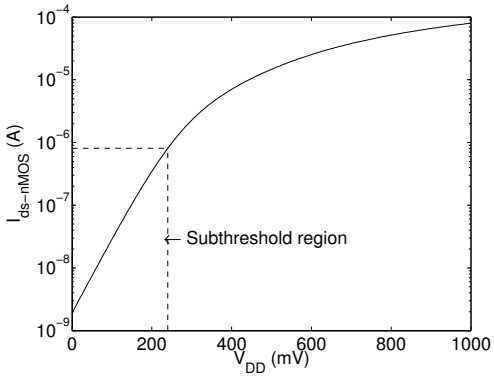


Fig. 1. nMOS transistor current I_{ds} as a function of V_{DD}, $V_{\mathrm{gs}} = V_{\mathrm{DD}}$

The average power consumption of a single CMOS gate can be expressed as [7]:

$$P_{\mathrm{dynamic}} = C_L V_{\mathrm{DD}}^2 P_{0\to1} f \tag{1}$$

where C_L is the gate's load capacitance, V_{DD} is the power supply voltage, f the clock frequency and $P_{0\to1}$ is the probability that charging of an internal node occurs. By reducing V_{DD} into the subthreshold region, quadratically reduction in the power consumption is achieved.

Operating circuits with power supply voltage below the transistor's threshold voltage is a dramatic way to reduce the power dissipation of circuits [8]. Transistors are said to operate in their subthreshold region when the supply voltage, V_{DD}, is decreased below the absolute value of the threshold voltage, $|V_t|$. In Fig. 1, the on-current going through a nMOS-transistor, I_{ds}, is plotted as the function of the power supply voltage, V_{DD}. As seen in the figure, the $I_{\mathrm{on}}/I_{\mathrm{off}}$ relationship can be reduced with as much as a factor of approximately 10^3 if V_{DD} is reduced from 1 V down to 150 mV. Reduced signal amplitude will be an advantage in a cryptography system as it makes it harder to measure side-channel information [2]. The reduction has a significant effect on the differential power analysis as well. The dynamic power consumption component is significantly reduced compared to the static

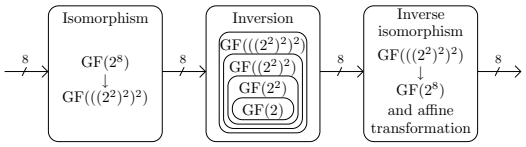


Fig. 2. S-box implementation

TABLE I
GATE COUNT

Design	Asynchronous	Pipelined
Logic gates	212	212
Sequencing gates	0	45
Total number of gates	212	257

power consumption when operating in the subthreshold region. These effects can be used to make it harder to detect the switching activity and thereby improving resistance against power analysis attacks with subthreshold operation [9].

It was shown in [10] how reduction in supply voltage reduces the current profile of an AES cryptographic processor. Subthreshold operation was used for increasing the DPA resistance in an 8-bit adder in [9]. This paper intend to investigate the use of subthreshold operation for increased protection against DPA attacks in an AES S-box implementation. The non-linear S-box operation is one of the major building block in the AES algorithm [11].

Different 8-bit adder designs were used for measuring the correlation between input data and instantaneous supply current in [12]. In [13], [14], floating gate techniques in combination with subthreshold operation were presented as a technique for increasing side-channel attacks resistance.

A brief introduction to subthreshold operation and side-channel attacks is given in this section. In Sec. II, the implementation of the S-box is described. A description of the test setup used in this paper is given in Sec. III. Simulation results are presented in Sec. IV and discussed in Sec. V. The contribution done in this work is summarized in Sec. V together with a conclusion.

II. S-BOX IMPLEMENTATION

The S-box operation consists of two operations. First, an inversion in the finite field GF(2^8) modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ is done. The second operation is an affine transformation $Y = AX^{-1} + b$, where A is a 8×8 fixed matrix and b is a 8×1 vector-matrix. A common way to optimize the S-box implementation is to use finite field arithmetic for transformation from $\mathrm{GF}(2^8)$ to $\mathrm{GF}(((2^2)^2)^2)$ [15]–[17]. In our implementation, the proposed implementation by Mentens *et al.* in [16] was used for a compact implementation of the S-box with the polynomial $P_x(x) = x^2 + x + \lambda$, $\lambda = zy$. Fig. 2 illustrates our implementation with conversion between fields and affine transformation.

The transformation matrix used is:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,1\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,1\,1 \\ 0\,0\,1\,0\,0\,1\,0\,0 \\ 0\,1\,0\,1\,0\,0\,1\,1 \\ 0\,1\,0\,0\,0\,1\,0\,1 \\ 0\,1\,0\,0\,0\,1\,0\,1 \\ 0\,1\,1\,1\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,0\,1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix}$$

where $a_i, b_i \in \mathrm{GF}(2)$ are the coefficients of $a \in \mathrm{GF}(2^8)$, $b \in \mathrm{GF}(((2^2)^2)^2)$. The resulting inverse transformation matrix with affine transformation is:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,1\,0\,0\,0\,0\,0 \\ 1\,1\,1\,0\,0\,0\,0\,0 \\ 1\,1\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,0\,1\,1\,1\,0 \\ 1\,0\,0\,1\,1\,1\,0\,0 \\ 0\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1\,0\,1\,0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

where $c_i, d_i \in \mathrm{GF}(2)$ are the coefficients of $c \in \mathrm{GF}(((2^2)^2)^2)$, $b \in \mathrm{GF}(2^8)$.

The constant multiplication with λ is implemented with 4 XOR gates [16]. Other multiplications are implemented using Mastrovito composite field multipliers [17] while additions are implemented using XOR-gates.

The implementation is done in a 90 nm process from STMicroelectronics with $V_{t,\mathrm{n}}$ = 0.24 V and $V_{t,\mathrm{p}}$ = -0.29 V, using a total of 164 C^{2}MOS XOR-gates and 48 AND-gates. A sense-amplifier based flip-flop [18] is used as the sequencing element. This flip-flop is able to drive a high load for a longer period of time and performs well in subthreshold operation [18]. An overview of the number of gates required in the implementation is given in Tab. I. Logic gates refer to arithmetic functions in the S-Box, while sequencing gates are number of overhead gates used for pipelining the circuit, i.e. flip-flops and clock buffers.

III. TEST SETUP

A circuit where the instantaneous supply current is uncorrelated to input signals is secure against side channel attacks [12]. For measuring the resistance against power analysis attack, the correlation between the input vector and the corresponding current drawn from the power supply has been calculated.

Fig. 3 shows the simulation test bench setup, based on the test bench from [12]. The power consumption of the S-box and the input drivers are taken into account, as well are the output loads. For each power supply voltage simulated, all possible 256 input combinations of the 8-bit signal are applied as input signals and the corresponding power consumption is measured as the current drawn from the power supply. Power consumption of S-box, input drivers and output loads are taken into account, as illustrated in Fig. 3.

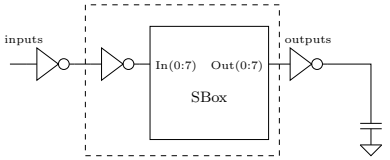
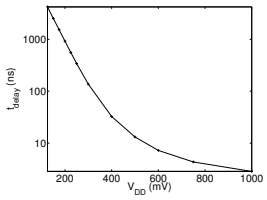
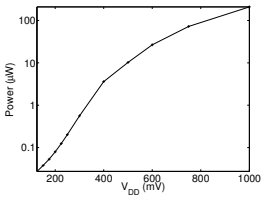


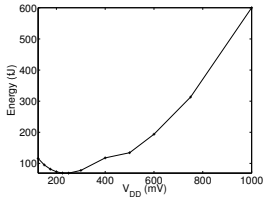
Fig. 3. Test bench setup



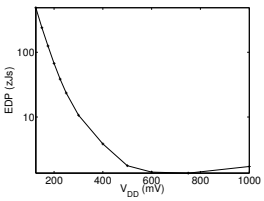
(a) Calculation time



(b) Power consumption

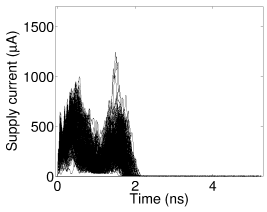


(c) Power-Delay Product (PDP)

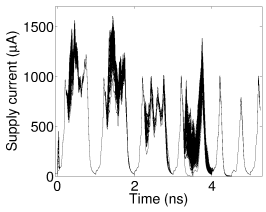


(d) Energy-Delay Product (EDP)

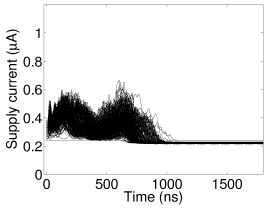
Fig. 4. Metrics of asynchronous S-box



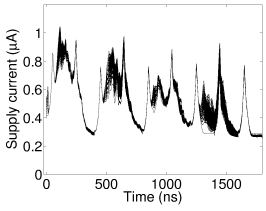
(a) Current drawn at $V_{\mathrm{DD}} = 1\,\mathrm{V}$, asynchronous S-box



(b) Current drawn at $V_{\mathrm{DD}} = 1\,\mathrm{V}$, pipelined S-box



(c) Current drawn at $V_{\mathrm{DD}} = 200\,\mathrm{mV}$, asynchronous S-box



(d) Current drawn at $V_{\mathrm{DD}} = 200\,\mathrm{mV}$, pipelined S-box

Fig. 5. Power consumption for all input combinations

TABLE II
SIMULATION RESULTS

Design	Calculation time	Throughput
Asynchronous 1 V	3.12 ns	2.56 Gbits
Pipelined 1 V	5.03 ns	6.36 Gbits
Asynchronous 200 mV	1085.64 n	7.37 Mbits
Pipelined 200 mV	1609.69 ns	19.88 Mbits

IV. SIMULATION RESULTS

The power supply voltage of the asynchronous S-Box implementation is stepped up from 125 mV to 1 V in Fig. 4. Performance metrics taken into account are the calculation time and average power consumption at maximum operation speed. The PDP and EDP values are also calculated and plotted. The lowest simulated PDP value is obtained when $V_{\mathrm{DD}} = 250\,\mathrm{mV}$ and is 68.8 fJ, while the lowest simulated EDP value is obtained when $V_{\mathrm{DD}} = 750\,\mathrm{mV}$ and is 1.36 zJs.

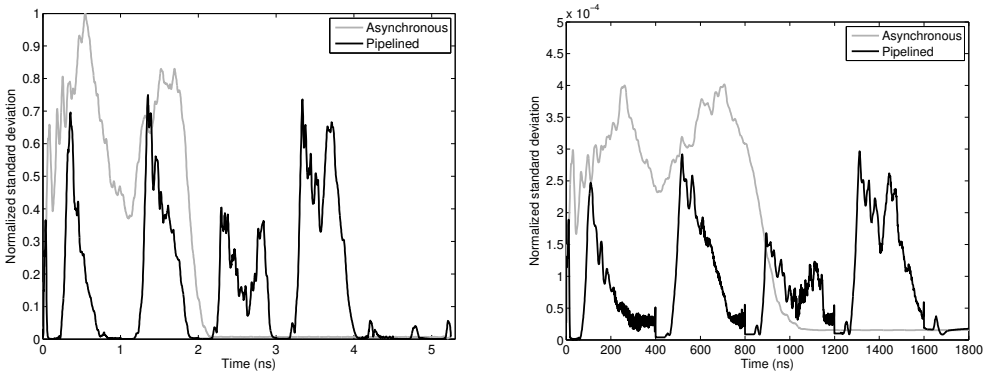
Fig. 5 shows the simulated instantaneous supply current in conventional superthreshold operation and subthreshold operation. Variations in supply current usage for different applied input vectors are clearly visible in the plots.

The standard deviation (std.) of the supply current is calculated in Matlab and normalized, such that the highest standard deviation value equals 1. The normalized std. is plotted in Fig. 6 for both values of V_{DD}. While the maximum normalized std. when operated at $V_{\mathrm{DD}} = 1\,\mathrm{V}$ equals 1, the maximum normalized std. is reduced to approx. 0.0004 in subthreshold operation.

V. DISCUSSION

Subthreshold operation reduces the standard deviation with a factor of 2500 according to Fig. 6(b). Although subthreshold operation offers increased resistance against power analysis attacks, circuits are not fully protected against attacks as long as there exists some correlation between the processed data and the instantaneous supply current. Subthreshold operation should be considered implemented together with other countermeasure techniques for improved resistance. Promising reported techniques include differential masking, random noise addition and blinding [6], [12], [19].

As subthreshold operation trades reduced power consumption against decreased operation speed, it is mainly applicable for ultra-low-power systems without high throughput requirements. Throughput in subthreshold circuits can be significantly improved by adding more pipeline stages to the circuit. Pipelining increases the throughput but does also increase the calculation time for individual bytes due to sequencing overhead delay. The power consumption increases as well when pipelining is introduced. The increased power consumption



(a) Standard deviation of $I_{\mathrm{V_{DD}}}$ at $V_{\mathrm{DD}} = 1\,\mathrm{V}$

(b) Standard deviation of $I_{\mathrm{V_{DD}}}$ at $V_{\mathrm{DD}} = 200\,\mathrm{mV}$

Fig. 6. Correlation between input values and power dissipation

should be taken into account when considering pipelining.

As the threshold voltage varies with process variations, subthreshold circuits are more sensitive to process variations compared to superthreshold circuits. Statistical process and temperature variation simulations as well as chip implementation would be instructive for verifying correct operation.

VI. Conclusion

This article presents a compact AES S-Box running in the subthreshold regime. Simulations indicate increased resistance against power analysis attacks with subthreshold operation. The correlation between power dissipation of different input values decreases with a factor of 2500 at the cost of 350 times delay degradation when applying subthreshold operation. The power consumption is 1.2 mW when operating at 1 V. When running at 200 mV, the power consumption is reduced to $0.13\,\mu$W.

Future works include analyzing the impact of process variations. Further gate-level optimizations are possible for reducing the total number of gates. This can be done with synthesis tools. For example, some of the AND gates can be replaced by NAND gates, offering smaller implementation [20]. Chip implementation of a complete cryptographic system should be considered for a more extensive analysis.

References

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proc. CRYPTO*, vol. LNCS 1109, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. CRYPTO*, vol. LNCS 1666, 1999, pp. 388–397.

[3] S. B. Örs *et al.*, "Power-analysis attack on an ASIC AES implementation," in *Proc. IEEE ITCC*, vol. 2, 2004, pp. 546–552.

[4] (2001) FIPS 197: Advanced Encryption Standard. National Institute of Standards and Technology. [Online]. Available: http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[5] K. Tiri *et al.*, "AES-based cryptographic and biometric security coprocessor IC in 0.18-μm CMOS resistant to side-channel power analysis attacks," in *Proc. IEEE VLSI Conference*, Jun. 2005, pp. 216–219.

[6] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Trans. Computer-Aided Design*, vol. 25, pp. 1197–1208, Jul. 2006.

[7] F.-X. Standaert *et al.*, "An overview of power analysis attacks against field programmable gate arrays," *Proc. IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.

[8] D. Liu and C. Svensson, "Trading speed for low power by choise of supply and threshold voltages," *IEEE J. Solid-State Circuits*, vol. 28, pp. 10–17, Jan. 1993.

[9] H. P. Alstad and S. Aunet, "Improving circuit security against power analysis attacks with subthreshold operation," in *Proc. IEEE DDECS*, 2008, pp. 12–13.

[10] G. F. Bouesse *et al.*, "A clock-less low-voltage AES crypto-processor," in *Proc. IEEE ESSCIRC*, 2005, pp. 403–406.

[11] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES SBoxes," in *Proc. CT-RSA*, vol. LNCS 2271, 2002, pp. 67–78.

[12] T. Sundström and A. Alvandpour, "A comparative analysis of logic styles for secure IC's against DPA attacks," in *Proc. IEEE Norchip*, Nov. 2005, pp. 297–300.

[13] B. Tongprasit and T. Shibata, "Power-balanced reconfigurable floating-gate-MOS logic circuit for tamper resistant VLSI," in *Proc. IEEE ISCAS*, 2006, pp. 4855–4858.

[14] O. Mirmotahari and Y. Berg, "Proposal for a ultra low voltage NAND gate to withstand power analysis attacks," in *Proc. World Academy of Science, Engineering and Technology*, vol. 25, Nov. 2007, pp. 83–87.

[15] A. Satoh *et al.*, "A compact Rijndael hardware architecture with S-Box optimization," in *Proc. ASIACRYPTO*, vol. LNCS 2248, 2001, pp. 239–254.

[16] N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, "A systematic evaluation of compact hardware implementations for the Rijndael S-Box," in *Proc. CT-RSA*, vol. LNCS 3376, 2005, pp. 323–333.

[17] T. Good and M. Benaissa, "Pipelined AES on FPGA with support for feedback modes (in a multi-channel environment)," *Information Security, IET*, vol. 1, pp. 1–10, Mar. 2007.

[18] H. P. Alstad and S. Aunet, "Three subthreshold flip-flop cells characterized in 90 nm and 65 nm CMOS technology," in *Proc. IEEE DDECS*, 2008, pp. 8–11.

[19] D. D. Hwang *et al.*, "Securing embedded systems," *IEEE Security & Privacy*, vol. 4, pp. 40–49, Mar. 2006.

[20] D. Canright, "A very compact s-box for AES," in *Proc. CHES*, vol. LNCS 3659, Aug. 2005, pp. 441–455.