ANALYSIS AND DETECTION OF POWER SIDE CHANNEL ATTACK

A Thesis in
Electrical Engineering
by
Navyata Gattu

© 2020 Navyata Gattu

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

May 2020
The thesis of Navyata Gattu was reviewed and approved* by the following:

Swaroop Ghosh
Assistant Professor
Thesis Advisor

Abhronil Sengupta
Assistant Professor

Kultegin Aydin
Department Head of EE and Professor
Head of the Department or Chair of the Graduate Program
Side Channel Attack (SCA) is a serious threat to the hardware implementation of cryptographic protocols. Various side channels have been explored to extract the keys, such as power, timing, electromagnetic emission and acoustic noise. Techniques proposed in literature to obfuscate such side channel signatures are often associated with design overheads and require reference data to be stored on chip. Machine Learning (ML)-based detection of SCA incurs high overheads of area and digitization which reduces their accuracy due to process variations of analog circuits and area. We propose a reference-free real-time power SCA detection technique using on-chip sensors. The dependency of phase/frequency of a 21-stage Ring Oscillator (RO) on supply voltage is exploited to detect the presence of a SCA resistance inserted at the power supply. The proposed detection mechanism is validated using simulation considering a detailed model of Power Distribution Network (PDN) and distributed power grid model. The proposed technique can detect even 1 ohm of resistance within 2 microseconds of attack initiation and incurs a tiny fraction of area and power (0.044% and 0.1065%, respectively) than existing techniques.
# TABLE OF CONTENTS

LIST OF FIGURES ........................................................................................................ vi

LIST OF TABLES ............................................................................................................ viii

ACKNOWLEDGEMENTS ................................................................................................. ix

Chapter 1 Introduction .................................................................................................. 1

1.1 Cryptographic algorithms ....................................................................................... 1
1.2 Power side channel attack ...................................................................................... 2
  1.2.1 Differential Power Analysis (DPA) ................................................................. 4
  1.2.2 Physical implementation .................................................................................. 5
1.3 Motivation ............................................................................................................... 6
1.4 Proposed idea ......................................................................................................... 7
1.5 SCA detection challenges ....................................................................................... 9
1.6 Conclusion ............................................................................................................. 10

Chapter 2 Power grid analysis ..................................................................................... 11

2.1 Power delivery network model .............................................................................. 11
2.2 Chip parameters .................................................................................................... 12
  2.2.1 Trend of area of chip with process technology ................................................ 13
  2.2.1.1 Impact of area of chip on number of $V_{dd}$ pins ........................................ 14
  2.2.1.2 Impact of area of chip on spacing of $V_{dd}$ pins ........................................ 14
  2.2.2 Trend of power consumption with process technology .................................. 15
  2.2.3 Trend of power consumption with process technology .................................. 16
2.3 Attack model .......................................................................................................... 17
2.4 Sensitivity analysis of $V_{\text{dro}p_{\text{sca}}}$ .................................................................... 21
  2.4.1 Impact of $SCA_{R}$ on $V_{\text{dro}p_{\text{sca}}}$ ................................................................. 21
  2.4.2 Impact of $I_{\text{load}}$ on $V_{\text{dro}p_{\text{sca}}}$ ................................................................. 23
  2.4.3 Combined impact of $I_{\text{load}}$ and $SCA_{R}$ on $V_{\text{dro}p_{\text{sca}}}$ ......................... 25
  2.4.4 Combined impact of $I_{\text{load}}$ and grid size on $V_{\text{dro}p_{\text{sca}}}$ ......................... 26
2.5 Conclusion ............................................................................................................. 27

Chapter 3 RO-based voltage sensor .......................................................................... 28

3.1 RO-based sensor design ....................................................................................... 28
3.2 $SCA_{R}$ model ..................................................................................................... 30
3.3 Qualitative analysis .............................................................................................. 30
  3.3.1 Impact of L and C parasitics of non-ideal $SCA_{R}$ ......................................... 32
  3.3.2 Proposed detection metric ............................................................................. 32
3.4 Quantitative analysis ............................................................................................ 33
3.5 Proposed detection mechanism .......................................................................... 33
  3.5.1 Obtaining $N_{\text{rising}}$ of RO ..................................................................... 34
LIST OF FIGURES

Figure 1-1: AES - 128.............................................................................................................2
Figure 1-2: Different types of side channels that can be monitored by adversary [6] ..........3
Figure 1-3: Distribution of power consumption as first S-box output; Distribution of power consumption for different LSBs of first S-box output [1] ......................... 3
Figure 1-4: DPA implementation [1]....................................................................................4
Figure 1-5: Physical implementation of power side channel attack ...................................5
Figure 1-6: Change in power grid impedance used as SCA detection metric in [9] .......... 6
Figure 1-7: LR ML model is employed to analyze the voltage variations of a power grid [10] ......................................................................................................................................7
Figure 1-8: Proposed RO-based detection technique ..........................................................8
Figure 1-9: Non-monotonic trend of \( N_{\text{rising}} \) for voltage and temperature variations .......9
Figure 2-1: PDN connected to distributed power grid .........................................................12
Figure 2-2: Chip area with technology .................................................................................13
Figure 2-3: Number of \( V_{\text{dd}} \) pins with technology [13][14][15] ....................................14
Figure 2-4: Intel Pentium 4 pin diagram .............................................................................15
Figure 2-5: Distance between \( V_{\text{dd}} \) pins with technology ................................................16
Figure 2-6: Power consumption with technology ...............................................................16
Figure 2-7: Load current per pin with technology .............................................................17
Figure 2-8: Power side channel attack model ....................................................................18
Figure 2-9: Heatmap of power grid indicating voltage drop due to SCA\(_R\) .....................19
Figure 2-10: Heatmap of power grid indicating voltage drop due to SCA\(_R\), in reality .... 19
Figure 2-11: Bump current distribution in absence/ presence of SCA\(_R\) .........................20
Figure 2-12: \( V_{\text{drop}_{\text{SCA}}} \) with SCA\(_R\) ............................................................................22
Figure 2-13: Victim and neighboring bump currents with SCA\(_R\) ....................................22
Figure 2-14: Bump current with load current; \( V_{\text{dropSCA}} \) with \( I_{\text{load}} \) ........................................23

Figure 2-15: Heatmap of power grid in absence/ presence of SCA\(_R\) of 1 \( \Omega \) with increasing load current. .................................................................24

Figure 2-16: Voltage drop at victim node with \( I_{\text{load}} \) and SCA\(_R\)...............................................25

Figure 2-17: Voltage drop at victim node with \( I_{\text{load}} \) and grid size ..............................................26

Figure 3-1: RO frequency with supply voltage \( V_{\text{dd}} \) .................................................................28

Figure 3-2: RO based voltage sensors connected to nodes of the power grid .............................29

Figure 3-3: Time delay between RO\(_{\text{clean}}\) and RO\(_{\text{SCA}}\) for SCA\(_R\) of 1 \( \Omega \) ......................29

Figure 3-4: \( \Delta \) Phase accumulation with \( N_{\text{rising}} \) .................................................................31

Figure 3-5: \( \Delta \) Phase with \( N_{\text{rising}} \) in presence of ideal/ non – ideal SCA\(_R\) .........................32

Figure 3-6: \( \Delta N_{\text{rising}} \) as a detection metric. .................................................................32

Figure 3-7: \( \Delta \) Phase with SCA\(_R\); \( \Delta N_{\text{rising}} \) with SCA\(_R\) ..................................................33

Figure 3-8: Proposed detection circuit ..................................................................................34

Figure 3-9: Placement of sensors at power nodes in a 3 x 3 power grid ..................................35

Figure 3-10: \( N_{\text{rising}} \) with temperature; \( \Delta N_{\text{rising}} \) with temperature .................................36

Figure 3-11: \( N_{\text{rising}} \) with \( V_{\text{dd}} \); \( \Delta N_{\text{rising}} \) with \( V_{\text{dd}} \) ............................................................37

Figure 3-12: \( N_{\text{rising}} \) with transistor sizing .............................................................................38

Figure 3-13: \( N_{\text{rising}} \) with threshold voltage ...........................................................................38

Figure 3-14: \( T_{\text{delay}} \) with \( N_{\text{rising}} \) in presence AC \( I_{\text{load}} \) .........................................................39

Figure 3-15: Reference based SCA detection using RO as a voltage sensor .........................40

Figure 3-16: \( N_{\text{rising}} \) with temperature; \( \Delta N_{\text{rising}} \) with temperature .................................41

Figure 3-17: \( N_{\text{rising}} \) with \( V_{\text{dd}} \) ......................................................................................42

Figure 3-18: Proposed detection circuit ..................................................................................43

Figure 3-19: \( N_{\text{clean}} \) with temperature .................................................................................44
LIST OF TABLES

Table 2-1: PDN and power grid parameters technique.......................................................... 12
Table 3-1: Proposed technique versus existing techniques...................................................... 45
ACKNOWLEDGEMENTS

I wish to pay my special regards to my advisor, Dr. Ghosh for guiding me persistently all through my master’s program. His continuous motivation, patience and immense knowledge helped me achieve my research goals.

I am grateful to my parents and family for being there for me and encouraging me constantly. This would have not been possible without their support. I also thank my fellow lab mates for helping me learn different things and mentoring me through out these two years.

This material is based upon work supported by the SRC (2847.001), NSF (CNS-1722557, CCF-1718474, CNS-1814710, DGE-1723687 and DGE-1821766) and DARPA Young Faculty Award (D15AP00089). Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the SRC, NSF and DARPA.
Chapter 1

Introduction

This chapter introduces cryptographic algorithms, power side channel attacks, their implementation, motivation to introduce an improved method of power SCA detection and a brief overview of the proposed method of detection. Additionally, the challenges faced during SCA detection are elaborated upon.

1.1 Cryptographic algorithms

Data security is important in all forms of computing [1]. Many cryptographic algorithms such as DES, AES, Blowfish, etc., have been introduced to encrypt data. In general, a cryptographic algorithm takes a plaintext as an input, operates on it with a key and gives a ciphertext as the output. For example, the AES-128 encrypts a 128-bit plaintext with a key of the same size over 10 rounds of operation (Figure 1-1). The plaintext is organized into a 4x4 matrix before being operated on by the AES.

Each round except for the 10th round, consists of 4 steps:

- **AddRoundKey**: A random key is exored with the plaintext state matrix. Each round has a different key.
- **SubBytes**: Each byte of the plaintext state is replaced by one from a lookup table called the substitution box or S-box. This table is standard for AES-128.
- **ShiftRows**: Bytes arranged in each row of the state matrix are shuffled.
- **MixColumns**: Using a linear operation, each of the columns of the bytes of the state matrix is mixed.

The last round is a special round in which only three of the four steps are performed.
The software implementations of these algorithms have been found to be slow, thereby warranting the need for hardware accelerators. The hardware implementations have shown great improvement in speed but are vulnerable to leakage of information through their side channels which can be attacked by the adversary [2]. The attacks exploit observable physical traits such as, timing [3], power consumption [4] and electromagnetic (EM) emanation [5] of the target implementation, which are related to underlying sensitive computation (Figure 1-2). A timing SCA attempts to extract the key by analyzing the time taken to execute cryptographic algorithms whereas power SCA targets the power consumption. CMOS devices also emit electro-magnetic emanation which is a function of the secret key during computation and can be leveraged to launch SCAs.

1.2 Power side channel attack

The output of every stage of the AES is dependent on the plaintext. Similarly, the AES consumes power differently depending on the plaintext that it needs to encrypt. Therefore,
for multiple plaintexts, the distribution of power consumption has a huge variation. To confirm this data dependency of power consumption, Figure 1-3 shows that the distributions of power consumption are different for different LSBs of the first S-box outputs.

Figure 1-2: Different types of side channels that can be monitored by adversary [6]

This data dependency of the power consumption is exploited by the adversary to carry out Simple Power Analysis (SPA), Differential Power Analysis (DPA) [7] or Correlation Power Analysis (CPA) [8] to extract the secret key. Although most SCAs require technical knowledge of the internal operation of the system, DPA-based power SCAs are also effective as black box attacks. Therefore, power SCAs can be very effective on a wide range of systems.
1.2.1 Differential Power Analysis (DPA)

The adversary targets the power consumption corresponding to AddRoundKey and SubBytes operations to extract the key. These output of these two operations can be represented by \( I_{i,n} = S[X_{i,n} \oplus K_n] \). The adversary leverages the byte wise nature of the AES operations to decipher the key byte wise which implies only 256 queries of the key byte need to be considered at a time. For different plaintexts, the I value for every query of the key byte is computed and a table is formed by the adversary. From the table, the adversary considers a selection bit based on which he separates out the power traces corresponding to each plaintext that he sends to the AES for every guess of the key byte. For example, if he chooses the LSB of I to be the selection bit, he creates two subsets based on 0 or 1 LSB of I. As shown in Figure 1-4, the adversary takes an average of each of the subsets of power traces.

\[
I_{i,n} = S[X_{i,n} \oplus K_n]
\]

Correct guess

Incorrect guess

Figure 1-4: DPA implementation [1]

Two cases follow this step:

- Correct guess: If he guessed the key byte correctly, then the averages of each of the subsets would approach the means of the separate distributions of 0 and 1 in Figure 1-3. The non-zero difference between these averages will lead to a DPA curve with clearly distinguishable peaks in it.
- Incorrect guess: If he guessed the incorrect key, the subsets would be a random
distribution of power traces whose means would have a zero difference between them.

This would result in a nil DPA curve.

Therefore, the adversary can clearly differentiate between the two cases based on the
DPA curve and extract the key byte wise.

1.2.2 Physical implementation

Power side channel attacks are performed by the adversary by means of physical probing
of the chip. He tampers with the wire bonds between the PCB and package and inserts a small
resistance across which the power signature is measured by an oscilloscope. He then sends
multiple plaintexts to the chip, from his computer and collects corresponding power waveform
data. With this data, he performs statistical analysis like DPA to extract the key. This poses a
huge threat to data security. Therefore, detection of the side channel attack resistance is essential
during runtime, so that measures can be taken to stop any further leakage of information.

![Figure 1-5: Physical implementation of power side channel attack](image)
1.3 Motivation

Existing works such as, [9] and [10] use Machine Learning (ML) techniques for power SCA detection. The technique proposed in [9] leverages the change in the impedance of the power grid due to the insertion of the $SCA_R$ at the power supply for detection (Figure 1-6). The chip’s power profiles with and without $SCA_R$s of various values are captured during the design phase. At runtime, ML compares the power profiles with the captured ones to detect SCA.

![Figure 1-6: Change in power grid impedance used as SCA detection metric in [9]](image)

In [10], a runtime detection technique is proposed that employs Logistic Regression (LR) ML model to analyze the voltage variations of a power grid (Figure 1-7). During the design phase, the Power Distribution Network (PDN) voltage variations are simulated in both secure and compromised environments and used for training the LR classifier. At runtime, the voltage variations induced due to SCA within a power grid are sensed by on-chip sensors and digitized by an Analog-to-Digital Converter (ADC), following which they are analyzed by the trained LR classifier to detect SCA.
Both techniques incur high area/power overheads due to the need for multiple on-chip sensors. Additionally, ADCs suffer from Integral Non-Linearity (INL) and Differential Non-Linearity (DNL) issues and incur high overheads due to large resistors/capacitors. ADCs are also sensitive to process variation, which results in decreased detection accuracy.

Also, they require reference data to be stored on chip, during the test phase. The accuracy of detection would depend on the resolution of the reference data. The higher the resolution, the more is the memory space required to store it. This results in an increased area overhead.

Therefore, it becomes vital to introduce a method of real time reference free SCA detection which is area and power efficient and does not need any digitization of data.

1.4 Proposed idea

We propose a high accuracy on-chip sensor for SCA detection. The overview of the proposed method is shown in Figure 1-8. The sensor includes a Ring Oscillator (RO) whose
oscillation frequency is a function of supply voltage. The number of rising edges of RO (N\text{rising}) over a period of time reduces if a SCA_R is introduced in the power grid. This feature is leveraged to detect the SCA. At runtime, the N\text{rising} of neighboring RO pairs is counted for every 2μs time window and compared with each other.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure1-8.png}
\caption{Proposed RO-based detection technique}
\end{figure}

If one of the ROs is connected to a node under attack, then the SCA is detected, based on the difference between the two N\text{rising} values. For example, when a chip with supply voltage V_{dd} of 1V and drawing a per pin load current of 1mA is attacked by an adversary by inserting 1Ω SCA_R on one of the nodes of the power grid (victim node), the V_{dd} at that node drops by ~1mV. Due to this drop, the RO at the victim node slows down by 67 ps per cycle and loses a total of 335ns over the detection time window. Consequently, the N\text{rising} is reduced by 40 edges, thereby indicating the presence of SCA_R. Note that the window of 2μs is chosen so that ΔN\text{rising} is large enough considering process and temperature variations for accurate detection. The detection accuracy of the proposed sensor is enhanced by a temperature sensor and calibration. Without the need for digitization of data, the area-intensive ADCs (also a source of inaccuracy) are eliminated. Also, the need for reference is eliminated, thereby reducing the area and complexity even further.
1.5 SCA detection challenges

- The detection mechanism needs to differentiate the frequency shift caused by SCA from other sources of phase shift. Therefore, a threshold $\Delta N_{\text{rising}}$ can be set, however, V/T variations can cause phase shifts of different magnitudes which can lead to an overall non-monotonic trend of the $\Delta N_{\text{rising}}$ as shown in Figure 1-9. The detection needs to calibrate out the V/T effect of the $\Delta N_{\text{rising}}$ to obtain a fixed threshold to rule out any possibility of false positives or negatives;

![Figure 1-9: Non-monotonic trend of N_rising for voltage and temperature variations](image)

- The detection technique should be capable of differentiating supply droop due to noise from that of SCA induced drop ($V_{\text{drop}_{\text{SCA}}}$) of equal magnitude to avoid false positives;

- A voltage bounce of same magnitude of $V_{\text{drop}_{\text{SCA}}}$ should not cancel the detection metric to avoid false negatives. The $N_{\text{rising}}$ in the absence of SCA i.e. $N_{\text{clean}}$ values are needed to compute $\Delta N_{\text{rising}}$;

- The $I_{\text{Chip}}$ can be noisy due to various transistors switching on and off at clock frequency. This can result in a noisy $V_{\text{drop}_{\text{SCA}}}$. The detection mechanism needs to be resilient to these variations. This work considers the above challenges to develop an area efficient, V/T resilient and highly accurate completely real-time on-chip SCA detection technique.
1.6 Conclusion

To sum up, the increasing vulnerabilities in ICs have increased the need for hardware security. One such vulnerability is the power signature of the IC, which can be used as a side channel to decipher cryptographic keys. These keys can be used by the adversary to decrypt data on chip. Therefore, detection of power side channel attacks becomes vital. The existing methods of detection use machine learning techniques. While these have high accuracy, they need reference data to be stored on chip and are area and power intensive due to their need for ADCs. The proposed idea overcomes these drawbacks, by using a low area ring oscillator based voltage sensor to sense the voltage drop at the power grid nodes when an SCA resistance is introduced by the adversary.
Chapter 2

Power grid analysis

This chapter focuses on modelling of power delivery networks of different chips, introducing the attack model, understanding variation of grid parameters under attack, determining a detection metric, and increasing the sensitivity of the detection metric to increase the ease of detection of SCA.

2.1 Power delivery network model

Figure 2-1 represents a detailed model of the power delivery network along with a distributed on-chip power grid [11]. The external source that serves as the $V_{dd}$ is connected to the off-chip part of the Power Delivery Network (PDN). The printed circuit board, package and the RLC ladder comprise this part. The decoupling capacitance along with the parasitic inductance and resistance are modelled as the RLC ladder $(RLC_s, p, pcb, pkg)$. The $V_{dd}$ and ground are distributed to different nodes of the chip via C4 bumps that are modelled as parallel RL interconnections $(R_{bump}, L_{bump})$ between the package and the chip. The on-chip distributed power grid is modelled as an RL network $(R_{grid}, L_{grid})$ with evenly distributed $V_{dd}$ and ground. The capacitance $C_{grid}$ represents the parasitic capacitance of the functional units connected to the grid. The values of the impedances as shown in Table 2-1 correspond to those of the Pentium 4 processor [12]. The loads are represented as dc current sources $I_{load}$ at every node of the power grid. A uniform load distribution across a 3x3 16 node grid is assumed for the analysis presented in future sections. A small grid size is considered for the sake of simplicity during analysis. The
load currents are chosen to be in the range of 0.1 mA to 200 mA to ensure a range of typical chip current values (Appendix B) have been considered.

Figure 2-1: PDN connected to distributed power grid [11]

Table 2-1: PDN and power grid parameters

<table>
<thead>
<tr>
<th>Impedance</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{s,pcb}/R_{p,pcb}/L_{pcb}/C_{p,pcb}$</td>
<td>0.094 mΩ/0.1666 mΩ/21 pH/240 µF</td>
</tr>
<tr>
<td>$R_{s,pkg}/L_{pkg}$</td>
<td>1 mΩ/120 pH</td>
</tr>
<tr>
<td>$R_{bump}/L_{bump}$</td>
<td>0.3 mΩ/0.5 pH</td>
</tr>
<tr>
<td>$R_{grid}/L_{grid}/C_{grid}$</td>
<td>50 mΩ/5.6 fH/0.12 nF</td>
</tr>
</tbody>
</table>

2.2 Chip parameters

For the sake of modelling the power grid close to that of a real chip, a detailed study on the trend of different parameters is needed. The previously introduced power grid model can
then be modified to match a range of power grids of chips from different process technology nodes.

### 2.2.1 Trend of area of chip with process technology

Transistors have gotten smaller with every technology node. This allows for more transistors to be incorporated on a given chip with fixed area, thus increasing the transistor density. Over the years, the demand for additional functionalities to be incorporated on chip has increased. This has increased the logic on chip, which has resulted in an increase in the area of the chip (Figure 2-2). While this may be counterintuitive as the transistor size is decreasing with technology, it should be noted that an implementation of an advanced chip like Intel Core i7 Ivy Bridge E would occupy almost 88 times more area when implemented using 180 nm technology as compared to its present technology i.e. 22nm.

![Figure 2-2: Chip area with technology](image-url)
2.2.1.1 Impact of area of chip on number of $V_{dd}$ pins

The density of the transistors on chip increases with advanced technology nodes, thereby increasing the number of loads on chip. This would result in the increase in number of $V_{dd}$ pins needed to be connected to the power grid, to support the high demand of the loads (Figure 2-3).

![Number of $V_{dd}$ pins vs technology](image)

Figure 2-3: Number of $V_{dd}$ pins with technology [13] [14] [15]

2.2.1.2 Impact of area of chip on spacing between $V_{dd}$ pins

The distribution of the $V_{dd}$ pins for Intel Pentium 4 is shown in Figure 2-4. For a given area, as the number of $V_{dd}$ pins increases, their density increases as well, which means they need to be very closely spaced. Therefore, the spacing between $V_{dd}$ pins decreases with technology (Figure 2-5).
2.2.2 Trend of power consumption with process technology

The increase in loads also results in large amounts of current drawn from the supply, which increases the power consumption of the chip with exception to advanced low power chips.
Figure 2-6: Power consumption with technology

like Atom, Atom Medfield, etc. (Figure 2-6). These chips are specifically designed to consume low power which may be needed in certain applications.

2.2.3 **Trend of load current with process technology**

As the load demand increases, the current drawn by each load also increases. Therefore, the per pin load current also proportionally increases (Figure 2-7).

To sum up, typical load currents of chips range from 0.3 mA to 200 mA. Larger chips used as desktop and laptop processors draw load currents > 20 mA while smaller chips used in embedded systems and low power processors like Intel ATOM draw currents < 10 to 20 mA.
It is important to model all these parameters during the power grid analysis, to have a precise understanding how they impact the SCA detection process. The load currents considered for analysis are of the typical range. The grid size is scaled by a scaling factor of the range 1 to 5 where 1 corresponds to 3x3 grid modelled using the parameters in table 2-1 and 5 correspond to those of AMD K10, which has the largest area in all the chips being listed in Appendix B.

2.3 Attack model

As mentioned in the introduction, the power signature of the chip serves as a side channel that can be used to decipher either a cryptographic operation taking place in the chip or the general working of the chip. An adversary can perform a power side channel attack on the chip by inserting probes at the interconnects between the PCB and package. He can tamper with the wire bumps by disconnecting them from the PCB and completing the circuit with probes. He would use the probes to monitor the power signature of the load connected to that node. The probes can be represented as a low resistance $\text{SCA}_R$ as shown in Figure 2-8. The node at which the adversary places the probes, is called the victim node. The drop across this resistance is $V_{\text{drop}_{\text{scA}}}$.
$V_{dd}$ is uniformly distributed across all nodes of the power grid, through the wire bumps. Any abnormality in a wire bump would cause a voltage drop in the node connected to it.

![Power side channel attack model](image)

**Figure 2-8:** Power side channel attack model

Therefore, in the presence of an $\text{SCA}_R$, the corresponding node connected to the wire bump under attack would experience a voltage drop and affect the loads connected to it.

When an $\text{SCA}_R$ of 1Ω is inserted at one of the bumps, the corresponding victim node should experience a voltage drop of 1mV if the load at that node draws a current of 1mA.

Therefore, the victim node voltage will become 0.999V in the case of a $V_{dd}$ of 1V, as shown in Figure 2-9.
While this may be expected, it is not true in the real situation. The actual power grid does not show a measurable drop in the victim node voltage (Figure 2-10).

The power grid is modelled such that all the nodes receive 1 V. For this to be possible, the drop across all the grid and bump impedances should be negligible so that almost no voltage is lost in distributing the $V_{dd}$ uniformly to all the nodes. Therefore, the overall impedance of the power grid and PDN is designed to be of the order of $m\Omega$ or lesser. An $SCA_R$ of 1 $\Omega$, is at least
1000 times larger than these impedances, thereby creating a high resistance path between the PCB and package.

If an equal load current of 1 mA is considered to be drawn at every node of the chip, then bump current distribution should be uniform as shown in Figure 2-11. This current distribution is disrupted when an SCA<sub>R</sub> is inserted at one of the bumps. The high impedance path due to the SCA<sub>R</sub> causes the load current corresponding to the victim node, to get divided and flow through the neighboring paths which almost act as short circuits due to their negligible impedance.

Therefore, there is a surge in the current in the neighboring branches while the victim branch current dips considerably. The excess current from the neighboring branches ultimately adds up and flows into the victim node. The negligible impedance of the grid connections aids in redistributing the victim node load current from the neighboring bumps to the victim node, thus ensuring the load at this node gets the current that it needs to draw.

In a network of resistors, increasing the total current, would proportionally increases the current flowing through the individual resistor branches. Therefore, in this case the load current can be increased to increase the $V_{\text{drop, sca}}$.

If increased to a measurable value, the $V_{\text{drop, sca}}$ causes a considerable drop in the victim node voltage $V_{\text{victim}}$ which would serve as a metric for detection of the SCA<sub>R</sub>. Further analysis
shows that this increase can be brought about by varying grid parameters like load currents and grid size.

2.4 Sensitivity analysis of $V_{\text{drop}_{\text{sca}}}$

As discussed previously, $V_{\text{drop}_{\text{sca}}}$ is affected by a number of factors like SCA$_R$, load current $I_{\text{load}}$ and grid size. This chapter highlights the impact of each of these factors on $V_{\text{victim}}$ and in turn, the detection of SCA$_R$. With the help of this sensitivity analysis, an optimal model for detection of SCA$_R$ can be proposed.

2.4.1 Impact of SCA$_R$ on $V_{\text{drop}_{\text{sca}}}$

Ideally, for a constant current flowing through a resistance, the voltage drop across it should increase with the increase in resistance. Therefore, it is expected that as SCA$_R$ increases for a constant bump current, the $V_{\text{drop}_{\text{sca}}}$ should also increase proportionally. As expected, Figure 2-12 shows that the $V_{\text{drop}_{\text{sca}}}$ increases with increase in SCA$_R$.

The increase in SCA$_R$ causes increase in the impedance of the victim bump branch, which results in decrease of the current flowing through it. This dip in current results in an increase in current flowing through the neighboring branches (Figure 2-13). Although the current flowing through the SCA$_R$ decreases, the increase in SCA$_R$, makes up for the dip in $V_{\text{drop}_{\text{sca}}}$.

Therefore, the $V_{\text{drop}_{\text{sca}}}$ increases with increase in SCA$_R$ in spite of the decrease in the branch current.
The change in branch currents with SCA$_R$ is very small in magnitude as the neighboring branches are of negligible resistance and even a 1Ω of SCA$_R$ would be large enough to force most of the current to flow through the neighboring branches completely.

Figure 2-12: $V_{\text{drop}_{\text{SCA}}}$ with SCA$_R$

Figure 2-13: Victim and neighboring bump currents with SCA$_R$
The negligible impedance of the power grid and the PDN largely aids the distribution of current to all the nodes irrespective of SCA_R. This works in the favor of the adversary to go undetected in the event of an attack.

### 2.4.2 Impact of $I_{\text{load}}$ on $V_{\text{drop}_{\text{Sca}}}$

In general, for a constant resistance, the voltage drop across it increases when the current flowing through it increases. Additionally, for a network of resistors, by virtue of current division, the increase in the total current would proportionally increase the current flowing through each of the branch resistors. Therefore, while the current flowing through the victim bump branch may be really small, the increase in the $I_{\text{load}}$ (Figure 2-14) would induce an increase onto it thereby increasing $V_{\text{drop}_{\text{Sca}}}$.

![Bump current vs load current](image1)

![$V_{\text{drop}_{\text{Sca}}}$ vs $I_{\text{load}}$](image2)

**Figure 2-14:** Bump current with load current; $V_{\text{drop}_{\text{Sca}}}$ with $I_{\text{load}}$

While this may be advantageous to the detection process, the increase in load current causes an increase in the branch currents of the power grid. There comes a point, beyond which the IR drop across the grid impedances becomes significant and causes a drop in all the grid node voltages, thereby making the power grid inefficient in distributing a perfect $V_{\text{dd}}$ supply as shown in Figure 2-15. Therefore, there exists a tradeoff between the ease of detection of SCA_R and
maintaining the grid node voltages at $V_{dd}$. In reality, circuits connected to the power grid on chip are designed to sustain a $V_{dd}$ drop of < 50 mV without having a negative effect on their timing parameters. The maximum voltage drop in node voltages caused when large load current of 100 mA flows through the grid is ~30 mV, which is well within the tolerable range of the circuits on chip. This voltage drop can be further reduced by decreasing the resistance between the nodes of the power grid. This can be done by decreasing the distance between the power pins.

![Image](135x193 to 512x546)

**Power grid node voltages with load current**

<table>
<thead>
<tr>
<th></th>
<th>0.1mA</th>
<th>100mA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0.1mA</th>
<th>100mA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0.1mA</th>
<th>100mA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Power grid node voltages in presence of $SCA_R$ of 1Ω**

<table>
<thead>
<tr>
<th></th>
<th>0.1mA</th>
<th>100mA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0.1mA</th>
<th>100mA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0.1mA</th>
<th>100mA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 2-15: Heatmap of power grid in absence/presence of $SCA_R$ of 1 Ω with increasing load current
2.4.3 Combined impact of $I_{\text{load}}$ and $SCA_R$ on $V_{\text{drop}_sca}$

In order to increase the $V_{\text{drop}_sca}$, the $I_{\text{load}}$ needs to be larger. In chips that consume more power, the loads draw larger currents which makes it easier to detect SCA$_R$. In lower power chips like Intel Atom, it gets tougher to detect SCA$_R$ as the current drawn per load of the chip is very small. The contours in Figure 2-16, indicate the voltage drop at the victim node. The brighter the contour, the more is the ease of detection of SCA. Therefore, it can be inferred that SCA detection is more possible in higher power consuming chips which would have higher load currents.

Additionally, the increase in SCA resistance, causes an increased voltage drop at the victim node, which further aids in detection. Although, it should be noted that the probes used by adversary may be mostly low resistance probes so that he goes undetected. Therefore, the detection should be made highly sensitive to low resistances. Figure 2-17 shows how the sensitivity of the detection technique can be increased for low resistance of 1 $\Omega$.

![Figure 2-16: Voltage drop at victim node with $I_{\text{load}}$ and $SCA_R$](image-url)
2.4.4 Combined impact of $I_{\text{load}}$ and grid size on $V_{\text{drop}_{\text{sca}}}$

The bump and grid resistances are scaled up in larger grids. This aids in detection of SCA at lower load currents itself as the drop at the victim node increases. Therefore, in larger chips it is possible to detect SCA for a larger range of load currents. It is still possible to detect SCA even in case of unequal distribution of loads, which causes some parts of the chip to have almost half the current of the maximum load current.

As the grid size decreases, the load current needs to be increased to detect SCA. This can be done periodically, for a short time to detect SCA while ensuring the power is not wasted. Workloads of the chip can be scheduled such that chip has a higher workload during the detection window. While this may be possible to a certain extent, it should also be noted that the current can only be increased till the maximum chip current rating, thus, limiting the ease of detection of SCA in these chips.

![Grid size vs $I_{\text{load}}$](image)

Figure 2-17: Voltage drop at victim node with $I_{\text{load}}$ and grid size
2.5 Conclusion

The power grid can be modelled to represent grids of processors of different technology nodes. The impact of SCA on different parameters such as the load current, bump current and the voltage drop at the victim node has been analyzed. The bump current in the victim bump gets diverted to its neighboring branches due to the high SCA resistance inserted in that branch, thereby reducing the drop at the victim node. Therefore, increasing the load current would increase this drop to a measurable value, thus increasing the ease of detection.

In the event of a power SCA attack on the chip, the voltage drop at the victim node will indicate it. By sensing the victim node voltage and comparing it with its neighboring nodes (which are not under attack), it can be detected that the chip is under attack. This information can be used to power off the chip or to take a measure to protect the signatures from being leaked.
Chapter 3

RO-based voltage sensor

The sensor needed to sense the voltage drop at the victim node should be (i) highly sensitive to voltage variations as low as a few millivolts; (ii) low in area as it needs to be connected to every node of the power grid; (iii) consume low power; (iv) should aid in detection of SCA within a small time window of few microseconds at the maximum so that the adversary does not go undetected; (v) should not disrupt the general functionality of the chip and should be completely noninvasive in sensing the drop in voltage.

A Ring Oscillator (RO) based voltage sensor is proposed as it meets all the above specified criteria. A detailed analysis of the behavior of the RO aids in designing a voltage sensor that is the most optimal for detection SCA_R.

3.1 RO-based sensor design

A RO is comprised of a chain of inverters connected in a loop fashion. The output of any of the inverters, is a signal oscillating at a frequency ‘f’. The RO frequency is affected by the

![Figure 3-1: RO frequency with supply voltage V_{dd}.](image)
supply voltage $V_{dd}$ given to the inverters. A decrease in $V_{dd}$ reduces the frequency of the RO (Figure 3-1). This voltage-frequency dependency of the RO makes it suitable to be used as a voltage sensor.

When connected to all nodes of the power grid, as shown in Figure 3-2, the RO outputs can be compared to detect any voltage drops that may be out of the tolerance range of regular voltage variations.

![Figure 3-2: RO based voltage sensors connected to nodes of the power grid](image)

![Figure 3-3: Time delay between $RO_{clean}$ and $RO_{SCA}$ for $SCA_R$ of 1Ω](image)
In the event of an attack, the RO at the victim node (RO_{SCA}) would slow down to a RO at an unaffected node (RO_{clean}) as shown in Figure 3-3.

The RO used in the sensor uses transistors with nominal Vt of 0.50V for nmos and -0.46V for pmos in 22nm predictive model. A 21-stage RO is considered with inverters (pmos/nmos has W/L of 4μm/0.03μm/2μm/0.03μm).

3.2 SCA_{R} model

In reality, the SCA_{R} used by the adversary includes parasitic inductance and capacitance that may affect the phase of the circuit response to a stimulus. Since the proposed detection technique is based on phase difference, it is necessary to consider the effects of these non-idealities. The parasitic components of the SCA resistance can be computed by 

\[ C_{\text{par}} = \frac{1}{2\pi f} \]  
\[ L_{\text{par}} = \frac{1}{4\pi^2 f^2 C_{\text{par}}} \]

where frequency \( f = \frac{1}{2\pi t_{n}}N \) is that frequency of clock on the chip (~1 GHz).

3.3 Qualitative analysis

The voltage drop caused at the victim node for a 1Ω SCA_{R} leads to a small RO frequency shift. To detect the SCA_{R}, the difference between the output of RO_{SCA} and RO_{clean} needs to be amplified. This small frequency shift results in a time delay, \( T_{\text{delay}} \) between the \( i^{th} \) rising edge of the RO_{SCA} and RO_{clean} as shown in Figure 3-3, where \( i = 1,2,3,...n \). \( T_{\text{delay}} \) and the corresponding phase difference \( \Delta \text{Phase}_{i} \) are calculated as shown in (2.1) and (2.2) respectively.

\[ T_{\text{delay}} = t_{\text{iSCA}} - t_{\text{iClean}} \]  \hspace{1cm} (2.1)

\[ \Delta \text{Phase}_{i} = \frac{T_{\text{delay}}}{t_{\text{iClean}}} \times 360 \]  \hspace{1cm} (2.2)

Every \( i^{th} \) cycle, \( T_{\text{delay}} \) increments such that \( t_{i+1} = t_{i} + \Delta t_{i} \). Therefore, \( T_{\text{delay}} \) is the total accumulated time difference from previous \( i-1 \) cycles. \( T_{\text{delay}} \) and the corresponding
\( \Delta \text{Phase}_i \) needs to be large enough to indicate the presence of SCA. The total accumulated phase difference at the end of the window is \( \Delta \text{Phase}_{n-1} \). However, the size of the detection window should be within the range of the typical time interval for which the adversary would keep the SCA inserted at the supply, to extract the crypto key. Based on simulations, a 2\( \mu \)s detection window is optimal to detect 1\( \Omega \) SCA\(_R\) without any false positives or false negatives as shown in Figure 3-4.

Each cycle of RO is delayed by time \( t_n \) due to each inverter. This delay accumulates to a value of \( C t_n \) over \( C \) cycles. Under SCA, the per stage delay would increase to \( t_n' = t_n + t_{n\text{SCA}} \) where \( t_{n\text{SCA}} \) is a measure of delay due to SCA\(_R\). This delay gets amplified by \( C \), over \( C \) cycles. Therefore, \( T_{\text{delay}} \) would evaluate to (2.3) and \( \Delta \text{Phase}_i \) to (2.4) respectively.

\[
T_{\text{delay}} = C t_n \text{SCA} \tag{2.3}
\]

\[
\Delta \text{Phase}_i = \frac{C t_n \text{SCA}}{T} \times 360 \tag{2.4}
\]

For example, the \( \Delta \text{Phase} = \Delta \text{Phase}_{n-1} \) at the end of 2\( \mu \)s, due to 1\( \Omega \) of SCA\(_R\) is 2897°.

Figure 3-4: \( \Delta \text{Phase} \) accumulation with \( N_{\text{rising}} \)
3.3.1 Impact of L and C parasitics of non-ideal SCA_R

Non-ideal SCA_R contains parasitic L and C. The capacitance (inductance) causes the voltage to lag (lead) from current. Therefore, the effects of the parasitic L and C on the voltage is almost cancelled out which implies that the ΔPhase caused by a non-ideal SCA_R is almost similar to that of an ideal SCA_R as shown in Figure 3-5.

![Figure 3-5: ΔPhase with N_rising in presence of ideal/ non-ideal SCA_R](image)

3.3.2 Proposed detection metric

While the phase difference caused due to an SCA_R as small as 1 Ω, is large enough to detect an attack, the direct use of a phase detector circuit to compare the outputs of the RO_SCA and

![Figure 3-6: ΔN_rising as a detection metric](image)
RO\textsubscript{clean}, may be complicated and cost ineffective.

The slowdown of RO also manifests in reduced number of rising/falling edges for a time window (Figure 3-6). Therefore, the number of rising edges (\(N_{\text{rising}}\)) of RO\textsubscript{clean} i.e. \(N_{\text{clean}}\) will be greater than that of RO\textsubscript{SCA} i.e. \(N_{\text{SCA}}\). The difference i.e. \(\Delta N_{\text{rising}} = N_{\text{clean}} - N_{\text{SCA}}\) is a good measure of \(\Delta\text{Phase}\).

For 1Ω SCA\textsubscript{R}, \(\Delta N_{\text{rising}}\) is 40 for a detection time window of 2\(\mu\)s. A simple counter and comparator can carry out detection without the need of costly phase detectors. Therefore, \(\Delta N_{\text{rising}}\) serves as a better metric for detection.

### 3.4 Quantitative analysis

\(V_{\text{drop SC}}\) increases with SCA\textsubscript{R} increasing the \(\Delta\text{Phase}\) and \(\Delta N_{\text{rising}}\) (Figure 3-7). An increase of roughly 15 edges in \(\Delta N_{\text{rising}}\) per ohm of SCA\textsubscript{R}. Therefore, detection accuracy/margin increases with higher SCA\textsubscript{R}.

![Figure 3-7: \(\Delta\text{Phase}\) with SCA\textsubscript{R}; \(\Delta N_{\text{rising}}\) with SCA\textsubscript{R}](image)

### 3.5 Proposed Detection Mechanism

The SCA detection (Figure 3-8) consists of three steps:

1. obtaining \(N_{\text{rising}}\) based on output of RO\textsubscript{SCA} and RO\textsubscript{clean}.
2. comparing the $N_{\text{rising}}$.

3. making decision if chip is under attack or not.

### 3.5.1 Obtaining $N_{\text{rising}}$ from RO

The ROs and counters are reset at the same time before every detection window. This ensures uniformity across all sensors. An $M$-bit counter (where $2^M - 1 \leq N_{\text{rising}}$) counts the $N_{\text{rising}}$ of the RO. To ensure that counting takes place for a fixed detection window of 2μs, the clock to the counter is gated by another signal of time period of the Detection Window (DW). The counter is reset before every detection window.

![Proposed detection circuit diagram](image)

**Figure 3-8:** Proposed detection circuit.

### 3.5.2 Comparison of $N_{\text{rising}}$ and decision making

The $N_{\text{rising}}$ from both the ROs is fed to the comparator and the output is saved in “SCA detected” register based on the condition shown in Figure 3-8. If $N_{\text{rising}} < N_{\text{clean}}$, the comparator...
outputs “1” (indicating SCA) else “0” (indicating normal operation). A buffer of ±2% is considered while making these comparisons to account for small variations due to chip conditions. Based on the SCA detection, the chip can be powered off or other protective measures could be invoked.

### 3.5.3 Placement of sensors

The ROs need to be placed at every power node of the grid i.e. nodes connected to the package, to distribute \( V_{dd} \) to all other nodes of the chip. To detect the SCA, the \( N_{\text{rising}} \) of two neighboring needs to be compared periodically. Therefore, the comparator and the SCA detection register can be shared between two neighboring ROs. Figure 3-9 shows the placement of sensors for a 3x3 power grid. The number of ROs needed, depends on the dimensions of the chip.

![Figure 3-9: Placement of sensors at power nodes in a 3 x 3 power grid](image)

Each RO would need its own counter and ‘and’ gate, which would be connected to a shared comparator. The comparator and the register are shared between two neighboring ROs. Therefore, for a chip having ‘n’ power pins, ‘n’ ROs, counters, ‘and’ gates and n/2 comparators, and registers would be needed for detection.
3.5.4 Resolution of detection

3.5.4.1 Impact of temperature

The degradation of carrier mobility of a MOSFET with temperature is higher than the increase in the gate overdrive due to lower threshold voltage. Therefore, the drain current decreases at higher temperature. Also, the increase in resistance of the SCA_R with increase in temperature causes a higher drop in $V_{dd}$ which slows down the RO decreasing the $N_{\text{rising}}$ in a fixed detection window (Figure 3-10). Consequently, $\Delta N_{\text{rising}}$ decreases with temperature as shown in Figure 3-10.

![Graph showing $N_{\text{rising}}$ and $\Delta N_{\text{rising}}$ vs temperature](image)

Figure 3-10: $N_{\text{rising}}$ with temperature; $\Delta N_{\text{rising}}$ with temperature

The uniform impact of temperature on the neighboring ROs would ensure that the effect of temperature is calibrated out when comparing their $N_{\text{rising}}$ values. Also, the $\Delta N_{\text{rising}}$ values though sensitive to temperature, will be still large enough to serve as a good metric to detect SCA_R without any false positives or negatives.

3.5.4.2 Impact of voltage

Figure 3-11 shows the $N_{\text{rising}}$ and $\Delta N_{\text{rising}}$ variation with $V_{dd}$. These parameters increase as the ROs have a higher frequency when $V_{dd}$ increases. The faster the ROs are, they gather more
edges in a fixed time window. This would imply that the difference between the edges of the two ROs $\Delta N_{\text{rising}}$ also increases.

The supply voltage variations at the source of the $V_{\text{dd}}$ will affect the entire chip uniformly. In the case of a droop, the voltage at a regular node on the power grid will drop by the magnitude of the droop and that at the victim node will drop by the sum of the droop voltage and the drop caused due to $\text{SCA}_R$. Similarly, in the case of the bounce, the asymmetry between the voltages at a clean node and a victim node will be unaffected. Therefore, the detection mechanism works independent of voltage variations.

3.5.4 Impact of RO sizing

The resistance of a MOSFET is inversely proportional its sizing $W/L$. Therefore, larger RO allows more drain current resulting in higher $N_{\text{rising}}$ in a fixed time window. The parasitic capacitance of MOSFET increases with the size of the MOSFET. This slows down the RO. Also, higher current drawn results in more drop across the $\text{SCA}_R$ reducing the effective supply voltage. This results in a slowdown of the RO and reduced $N_{\text{rising}}$ as shown in Figure 3-12. The higher current also results in a higher $V_{\text{drop}_{\text{SCA}}}$, thereby increasing $\Delta N_{\text{rising}}$ enhancing the sensitivity of the detection.
3.5.4.4 Impact of threshold voltage

Figure 3-13 shows that the increasing trend in $N_{\text{rising}}$ with decreasing threshold voltage $V_t$ of the RO transistors. Therefore, a low $V_t$ (LVT) RO is more sensitive to SCA compared to a normal $V_t$ (NVT) and high $V_t$ (HVT) RO.
3.5.4.5 Impact of AC $I_{load}$

In reality, at least 10-20% of the transistors on chip toggle at the clock frequency which reflects in the current drawn by the chip. The proposed RO-based detection method works even when $I_{load}$ is an AC current toggling at clock frequency of 1 GHz with an amplitude 100 μA and a DC component of 1mA (Figure 3-14). This is because the average drop at the victim node caused due to the SCA, remains constant irrespective of the instantaneous variations in the load current.

![Figure 3-14: $T_{delay}$ with $N_{rising}$ in presence AC $I_{load}$](image)

3.6 Alternate reference based approach

Recording typical RO values of $N_{rising}$ (in the absence of SCA) during test phase and storing on chip would also serve as a good reference to compare the real time $N_{rising}$ values with. As opposed to [9] [10], a method to optimize the way the reference data has been introduced in this approach. Therefore, the memory overhead compared to the ML techniques would be reduced by a huge percentage. A detailed analysis of this approach has been done to understand the advantages of a reference free approach over a reference based approach with the same RO based voltage sensor and how both the above techniques are better than the ML techniques.
3.7 Reference based SCA detection

As discussed earlier, the storage of a reference for \(N_{\text{rising}}\) on chip could be one of the approaches for detection (Figure 3-15).

Previously, two ROs on chip were compared to detect SCA. In this method, the RO output is compared with the test phase data to achieve the same goal. It becomes crucial to ensure the same level of uniformity between the conditions under which the data from both the parties involved are compared. Therefore, it becomes important to account for the temperature and voltage variations experienced by the RO in real time and ensure that the reference data is also corresponding to the same conditions.

3.7.1 Resolution of detection

The resolution of detection of this method remains the same as the previous method i.e. a \(\Delta \text{Phase} = 2897^\circ\) and \(\Delta N_{\text{rising}} = 40\) edges accumulates over a detection window of 2\(\mu\)s, due to 1\(\Omega\) of \(\text{SCA}_R\). The impact of temperature, voltage, RO sizing and threshold voltage remain the same as well. Although the need to store reference data \(N_{\text{clean}}\) corresponding to different conditions, makes it important to consider the variations of \(N_{\text{rising}}\) with temperature and voltage and explicitly calibrate them out.
3.7.1.1 Impact of temperature

A large variation in $\Delta N_{\text{rising}}$ with temperature (Figure 3-16) makes it difficult to set a $\Delta N_{\text{rising}}$ threshold that clearly differentiates the effects of an SCA from temperature variations. This variation can be reduced by calibrating out the effects of temperature. One approach is to reduce the detection window such that the excess edges counted due to decrease in temperature are calibrated out. The detection window needs to be increased at higher temperatures to allow more time for edges to be captured to compensate for the temperature-induced extra delay. This can be done by making the DW temperature sensitive to obtain a fixed threshold of 74 edges for a $V_{dd}$ of 1V over a temperature range of -10°C to 90°C as shown in Figure 3-16. This approach overcomes the challenges of setting a fixed threshold and differentiating between the effects of temperature changes and SCA.

3.7.1.2 Impact of voltage

The RO frequency increases with voltage which results in more edges in a given time window as shown in Figure 5-3.
While this may be beneficial, it may lead to false negative SCA detection since extra edges due to voltage variations can hide the effect of SCA. Simulations results show that the difference in $N_{\text{rising}}$ between SCA-free ROs running at two different voltages is at least 5 times larger than $\Delta N_{\text{rising}}$ (denoted by $\delta$ in Figure 3-17) for a given voltage, eliminating the possibility of false negatives.

### 3.8 Proposed detection mechanism

The SCA detection (Figure 3-18) consists of three steps (i) obtaining $N_{\text{rising}}$ based on RO output; (ii) computation of expected $N_{\text{clean}}$ values; (iii) comparison of $N_{\text{rising}}$ with $N_{\text{clean}}$ and deciding if the chip is under attack or not.

While step (i) is the same as the previous method, step 2 is different in the sense that data for all possible conditions of the chip should be recorded and stored from the test phase. The impact of temperature and voltage variations become important in this case.
### 3.8.1 Computation of $N_{\text{clean}}$

Figure 3-18 shows that the $N_{\text{rising}}$ are highly sensitive to temperature and have a large difference of 4030 edges over a temperature range of $-10^\circ\text{C}$ to $90^\circ\text{C}$. For accurate SCA detection the $N_{\text{clean}}$ corresponding to all possible temperatures need to be recorded and stored on chip during the test phase. This increases the area over head of the detection mechanism as the accuracy of detection would be dependent on how granular is the temperature range over which the data would be recorded. With such a large variation in $N_{\text{rising}}$ it becomes crucial to keep the granularity of the data at a maximum i.e. the data should be recorded at very small temperature intervals. This would mean the memory needed for storing $N_{\text{clean}}$ would increase by a lot.

Therefore, it makes more sense to compute $N_{\text{clean}}$ whenever needed.

During the test phase, $N_{\text{clean}}$ values for a given $V_{dd}$ can be recorded for temperatures ranging from $-10^\circ\text{C} \leq T \leq 90^\circ\text{C}$. These values are used to obtain a polynomial (2.5).

$$N_{\text{clean}}|_{V = V_{dd}} = a_2 T^2 + a_1 T + a_0$$  \hspace{1cm} (2.5)
For computing $N_{\text{clean}}$ at run-time, we require three 32-bit registers storing the coefficients $(a_2, a_1, a_0)$ of the polynomial, 3 multipliers and 2 adders. The dynamic temperature value $T$ is sensed from the on-chip temperature sensor for computing $N_{\text{clean}}@T$. We have chosen a polynomial of degree 2 (yielding 3 coefficients) since that allows us to accurately compute $N_{\text{clean}}$ at run-time within our chosen detection window. In our case, during test phase, we record the $N_{\text{clean}}$ values at $V_{dd} = 1\text{V}$ and a temperature range of $-10^\circ\text{C}$ to $90^\circ\text{C}$ in steps of $10^\circ\text{C}$. The corresponding polynomial coefficients that can be used for computing $N_{\text{clean}}$ at run-time are $a_2 = 0.2$, $a_1 = -59.4$ and $a_0 = 6329.3$, that ensure a close fit to the actual curve of $N_{\text{clean}}$ as shown in Figure 5-5.

The accuracy of the polynomial coefficients can be increased by sampling $N_{\text{clean}}$ values at finer-grained temperature values, but this increases test time as each sample needs $2\mu\text{s}$ to be recorded. Furthermore, a higher degree of polynomial can be chosen at test time for higher accuracy of $N_{\text{clean}}$ computation at run-time. However, this incurs increased area and power overhead. It should be noted that the polynomial degree accuracy is bounded by the computation time since it is limited by the chosen detection window. Therefore, a trade-off is required between accuracy, area, power consumption and test time for the reference-based detection technique.

Figure 3-19: $N_{\text{clean}}$ with temperature.
### 3.9 Comparative Analysis

This section compares the proposed SCA sensor with [9] and [10] (Table 3-1), based on parameters such as area, power, number of sensors needed, methodology, detection metric and need for reference data.

Table 3-1: Proposed technique versus existing techniques.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Methodology</td>
<td>LR ML classification</td>
<td>LR ML classification</td>
<td>RO Voltage dependence</td>
<td>RO Voltage dependence</td>
</tr>
<tr>
<td>Need to store reference data on chip</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Detection time</td>
<td>6.6μs</td>
<td>394ns (w/ 85MHz Clk)</td>
<td>2μs</td>
<td>2μs</td>
</tr>
<tr>
<td>Detection metric</td>
<td>Power signature</td>
<td>Voltage variations across power grid</td>
<td>ΔPhase</td>
<td>ΔPhase</td>
</tr>
<tr>
<td>Minimum SCA_R</td>
<td>1Ω</td>
<td>Unknown</td>
<td>1Ω</td>
<td>1Ω</td>
</tr>
<tr>
<td>Technology</td>
<td>45nm</td>
<td>45nm</td>
<td>22nm</td>
<td>22nm</td>
</tr>
<tr>
<td>ADC</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Area (kGE)</td>
<td>44444</td>
<td>749.62</td>
<td>19.58</td>
<td>1.9286</td>
</tr>
<tr>
<td>Power (mW)</td>
<td>94</td>
<td>-</td>
<td>3.9104</td>
<td>0.1001</td>
</tr>
<tr>
<td>Number of sensors used</td>
<td>Depends on grid size</td>
<td>Depends on grid size</td>
<td>1</td>
<td>Depends on grid size</td>
</tr>
</tbody>
</table>

1. the ML based detection techniques create an SCA aware environment during test phase of the chip to train the LR classifier. Both the reference free and reference based SCA detection techniques exploit the inherent RO frequency shift under SCA which serves as a real-time detection metric;

2. the chip’s power signature data and N_clean values needs to be stored in the memory for [9,10] and the reference-based approach respectively, while this is not required for the reference free approach.
3. the reference-based detection is simple with only a single instance of the sensor needed to achieve the same accuracy that is achieved by multiple instances of the LR model-based detection [9,10] and the reference free approach;

4. the area and power of the reference free detection mechanism is 0.043% and 0.1065% of [10] respectively, and that of the reference-based detection mechanism is 0.0441% and 2.6% (compared in kGE where 1kGE = 60000F² where F = technology [16]). GE is the area of NAND2 gate equivalent. ADCs contribute to more than 90% of the area and power of the ML based techniques. The proposed detection techniques eliminate the need of digitization resulting in a design that is free of area and power overheads of an ADC;

5. the proposed methods are scalable to resistances lower than 1Ω provided that the detection window is increased. However, increasing the detection window results in increased area and power overheads.

3.10 Conclusion

To sum up, two models were proposed for SCA detection. The reference free model detected SCA based on \( \Delta N_{\text{rising}} \) between two neighboring R\( \text{os} \), used as voltage sensors to detect the voltage drop at the victim node. This is done during run time and needs a detection window of 2 \( \mu \text{s} \) to detect an SCA as low as 1 Ω. The reference based method detects SCA based on \( \Delta N_{\text{rising}} \) between the prestored \( N_{\text{clean}} \) values (from the test phase), and the RO at a node on the power grid. Similar to the reference free method, this is done during run time and requires a detection window of 2 \( \mu \text{s} \) to detect an SCA as low as 1 Ω. The reference free method proves to better than [9,10] and the reference based SCA detection method, in most aspects. Although, the number of sensors needed for this method depends on grid size, the total area needed for the entire set up would still be less than its counterparts.
Chapter 4

Discussion

This chapter discusses the limitations of both proposed methods. Additionally, their testing overheads and behavior in presence of noise has been elaborated.

4.1 Reference free SCA detection

4.1.1 Limitations

In case of small chips with less current consumption of few mA, the ease of detection would not be favorably high. This would lead to false negatives. The approaches to overcoming this limitation would be:

- To increase the load currents for the length of the detection window in order to increase the sensitivity of detection of drop at the victim node. This can be done by scheduling specific workloads during chip run time, such that the loads draw more current. Although this should be done with caution so as to minimally disrupt the functioning of the chip and to avoid increased power consumption for long periods of time.

- To increase the length of detection window so that higher number of $N_{\text{rising}}$ can be sampled and compared. It should be noted that the length detection window should always be shorter than the typical time duration for which the adversary monitors the power signature.

4.2 Reference based SCA detection

4.2.1 Limitations

- Errors due to sampling clock phase: The sampling clock DW may have skew and phase of its own which may give rise to error in counting of $N_{\text{rising}}$ as some edges may be lost or gained
if the $|\text{skew}| >$ time period of RO. This may be a source of inaccuracy and may offset $N_{\text{rising}}$ by a few edges, which may cause an error within 1% margin of $N_{\text{clean}}$. The possibility of false positives can be reduced by ensuring that the error margin is 1-2%.

- **Impact of aging:** The aging of transistors in the RO would result in decreased $N_{\text{rising}}$. This would give rise to false positive detection as the polynomial coefficients were computed in test phase based on the $N_{\text{clean}}$ values at that particular time. [17] can be used to calibrate out the effects of aging from the RO to make the detection resilient to aging.

4.2.2 **Detection in noisy supply current**

Similar to the reference free approach, the voltage sensors detect the drop in voltage due to SCA in the presence of loads toggling at clock frequency.

4.2.3 **Testing phase overheads**

The proposed RO-based SCA detection methodology depends on the data collected during test phase, which is used to build a model for comparison with the real-time data. There is a trade-off between accuracy and test time (as discussed in Section 2.3.2). The regular per-chip test time is 2.29s [18]. The additional test time required per chip to obtain $N_{\text{clean}}$ values is 22μs if the values are recorded in temperature intervals of 10°C. Even if the temperature interval is reduced to 1°C (for increased accuracy), the time required to obtain $N_{\text{clean}}$ increases to 0.2 ms which is still less than 0.01% of the regular test time.

4.2.4 **Detection in DVFS capable chips**

If a chip needs to be operated at multiple voltages, then multiple equations for $N_{\text{clean}}$ computation are required. For example, if the proposed technique needs to be implemented on a chip with DVFS capability, then we need separate equations for $N_{\text{clean}}$ for each voltage mode.
This increases the total number of coefficients to be stored for all the equations, resulting in higher area overhead. Also, the test time increases by a factor of the number of voltage modes.

4.3 Conclusion

Ease of detection in smaller chips will be lesser due to small load currents. This limitation can be overcome by increasing the detection window, to capture a greater number of rising edges and to increase the $\Delta N_{\text{rising}}$. Additionally, the load currents on chip, may toggle at the clock frequency. Both the approaches have been shown to be successful in detecting SCA in spite of toggling load currents. The test time overheads of the reference based SCA detection method have been accounted for as 22$\mu$s and this test time increases with the number of voltage levels that are needed, in case of implementation on a DVFS capable chip.
Chapter 5

Conclusion and future work

Power side channel attacks on chips by physically probing the PCB to package interconnects is a serious security threat. These attacks need to be detected so that measures can be taken to protect the chip from further information leakage during run time. Existing methods use ML techniques to detect SCA. While they may be accurate, they have limitations which were overcome by the proposed detection technique.

Two approaches were explored for SCA detection using a RO based voltage sensor: the reference free approach and reference based approach. The reference free approach was proven to be the better approach for detection, in terms of area, power and complexity. It provides a full proof way of detection. Though the reference-based approach may not be as efficient as this approach, it is surely better than its existing counterparts [9] [10].

The hardware implementation of the proposed set up will be explored as a part of future work. Additionally, further study on how to increase the sensitivity of detection in smaller chips will be explored.
Appendix A

Glossary

SCA\textsubscript{R} \hspace{1cm} \text{Side channel resistance}

RO\textsubscript{clean} \hspace{1cm} \text{RO at a node that is not under attack}

RO\textsubscript{SCA} \hspace{1cm} \text{RO at a node that is under attack (victim node)}

T_{i\text{delay}} \hspace{1cm} \text{Time delay between } i^{\text{th}} \text{ rising edge of } RO\textsubscript{SCA} \text{ and } RO\textsubscript{clean}

\text{t}_{i\text{SCA}} \hspace{1cm} \text{Time instance of } i^{\text{th}} \text{ rising edge of } RO\textsubscript{SCA}

\text{t}_{i\text{clean}} \hspace{1cm} \text{Time instance of } i^{\text{th}} \text{ rising edge of } RO\textsubscript{clean}

\text{t}_{n} \hspace{1cm} \text{Time delay of an inverter}

\text{t}_{n\text{SCA}} \hspace{1cm} \text{Time delay due to } SCA\textsubscript{R}

\Delta\text{Phase}_{i} \hspace{1cm} \text{Phase difference between } i^{\text{th}} \text{ rising edge of } RO\textsubscript{SCA} \text{ and } RO\textsubscript{clean}

\Delta\text{Phase}_{n-1} \hspace{1cm} \text{Total accumulated phase difference at the end of the detection window}

\Delta\text{Phase} \hspace{1cm} \text{Total accumulated phase difference at the end of the detection window}

\text{Non-ideal SCA}\textsubscript{R} \hspace{1cm} SCA\textsubscript{R} \text{ with parasitic L and C}

\text{N}_{\text{rising}} \hspace{1cm} \text{Number of rising edges in RO output, counted within a fixed detection window}

\text{N}_{\text{clean}} \hspace{1cm} \text{Number of rising edges in } RO\textsubscript{clean} \text{ output, counted within a fixed detection window}

\text{N}_{\text{SCA}} \hspace{1cm} \text{Number of rising edges in } RO\textsubscript{SCA} \text{ output, counted within a fixed detection window}
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>GE</td>
<td>Gate Equivalent is a technology independent unit of measure</td>
</tr>
<tr>
<td>$\Delta N_{\text{rising}}$</td>
<td>Difference in $N_{\text{rising}}$ of $ RO_{\text{clean}}$ and $ RO_{\text{SCA}}$</td>
</tr>
<tr>
<td>$V_{\text{drop}_{\text{SCA}}}$</td>
<td>Voltage drop across the $SCA_R$</td>
</tr>
<tr>
<td>$I_{\text{load}}$</td>
<td>Current drawn by a load connected to a node on the power grid</td>
</tr>
<tr>
<td>Bump current</td>
<td>Current passing through $RL_{\text{bump}}$ branches that connect the package to the nodes on the chip power grid</td>
</tr>
<tr>
<td>Victim bump</td>
<td>Bump branch in which the $SCA_R$ is inserted</td>
</tr>
<tr>
<td>Victim node</td>
<td>Power grid node that is under attack</td>
</tr>
<tr>
<td>$V_{\text{victim}}$</td>
<td>Victim node voltage</td>
</tr>
</tbody>
</table>
Appendix B

Chip parameters [13][14][15]

*These values are ballpark figures calculated based on assumption that $V_{dd}$ pins are uniformly distributed on chip.

<table>
<thead>
<tr>
<th>Chip</th>
<th>Application</th>
<th>Technology</th>
<th>Area (mm²)</th>
<th>Total number of pins</th>
<th>Number of $V_{dd}$ pins</th>
<th>Distance between $V_{dd}$ pins* (mm)</th>
<th>Power consumption (W)</th>
<th>$V_{dd}$ (V)</th>
<th>Total current consumption (A)</th>
<th>Per pin current consumption $I_{load}$* (mA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARM 1</td>
<td>Embedded systems</td>
<td>3µm</td>
<td>50</td>
<td>90</td>
<td>8</td>
<td>7.07</td>
<td>1</td>
<td>1.8</td>
<td>555.55</td>
<td>6</td>
</tr>
<tr>
<td>Pentium</td>
<td>Desktop processor</td>
<td>0.8 µm</td>
<td>294</td>
<td>320</td>
<td>48</td>
<td>1.558</td>
<td>8.1 - 15.5</td>
<td>3.6</td>
<td>29.16 - 55.8</td>
<td>91.12 - 174.37</td>
</tr>
<tr>
<td>Pentium Pro</td>
<td>Desktop processor</td>
<td>0.6 µm</td>
<td>307</td>
<td>387</td>
<td>70</td>
<td>1.001</td>
<td>29.2 - 36.9</td>
<td>3.3</td>
<td>8.8485 - 11.18</td>
<td>22.9 - 28.9</td>
</tr>
<tr>
<td>AMD K5</td>
<td>Desktop processor</td>
<td>0.35 µm</td>
<td>251</td>
<td>296</td>
<td>53</td>
<td>0.2141</td>
<td>11.8 - 15.8</td>
<td>3.6</td>
<td>3.278 - 4.388</td>
<td>11.07 - 14.82</td>
</tr>
<tr>
<td>Chip</td>
<td>Application</td>
<td>Technology</td>
<td>Area (mm²)</td>
<td>Total number of pins</td>
<td>Number of $V_{dd}$ pins</td>
<td>Distance between $V_{dd}$ pins* (mm)</td>
<td>Power consumption (W)</td>
<td>$V_{dd}$ (V)</td>
<td>Total current consumption (A)</td>
<td>Per pin current consumption $I_{load}^*$ (mA)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>------------</td>
<td>----------------------</td>
<td>-------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------</td>
<td>------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Pentium II Klamath</td>
<td>Desktop processor</td>
<td>0.35 µm</td>
<td>195</td>
<td>242</td>
<td>27</td>
<td>0.2308</td>
<td>38.4 - 43</td>
<td>3.3</td>
<td>11.63 - 13.03</td>
<td>48.08 - 53.84</td>
</tr>
<tr>
<td>Pentium III Coppermine</td>
<td>Desktop processor</td>
<td>0.18 µm</td>
<td>80</td>
<td>242</td>
<td>75</td>
<td>0.14783</td>
<td>16 - 39.55</td>
<td>3.3</td>
<td>4.84 - 11.98</td>
<td>20.03 - 49.52</td>
</tr>
<tr>
<td>Pentium 4 Northwood</td>
<td>Desktop processor</td>
<td>0.13 µm</td>
<td>145</td>
<td>478</td>
<td>85</td>
<td>0.10076</td>
<td>89</td>
<td>1.475</td>
<td>60.338</td>
<td>126.23</td>
</tr>
<tr>
<td>AMD Athlon XP</td>
<td>Desktop processor</td>
<td>0.13 µm</td>
<td>193</td>
<td>462</td>
<td>105</td>
<td>0.12028</td>
<td>48.5 - 68.3</td>
<td>1.65</td>
<td>29.39 - 41.39</td>
<td>63.6 - 89.5</td>
</tr>
<tr>
<td>Pentium 4 Prescott</td>
<td>Desktop processor</td>
<td>90 nm</td>
<td>110</td>
<td>478</td>
<td>85</td>
<td>0.08776</td>
<td>89 - 115</td>
<td>1.4</td>
<td>63.57 - 82.14</td>
<td>132.9 - 171.8</td>
</tr>
<tr>
<td>AMD K10</td>
<td>Desktop processor</td>
<td>65 nm</td>
<td>283</td>
<td>939</td>
<td>105</td>
<td>0.07166</td>
<td>95</td>
<td>1.4</td>
<td>67.85</td>
<td>72.26</td>
</tr>
<tr>
<td>Chip</td>
<td>Application</td>
<td>Technology</td>
<td>Area (mm²)</td>
<td>Total number of pins</td>
<td>Number of V_{dd} pins</td>
<td>Distance between V_{dd} pins* (mm)</td>
<td>Power consumption (W)</td>
<td>V_{dd} (V)</td>
<td>Total current consumption (A)</td>
<td>Per pin current consumption I_{load}^* (mA)</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------</td>
<td>------------</td>
<td>------------</td>
<td>----------------------</td>
<td>-----------------------</td>
<td>-----------------------------------</td>
<td>-----------------------</td>
<td>-----------</td>
<td>--------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Intel core i7</td>
<td>Desktop processor</td>
<td>45 nm</td>
<td>263</td>
<td>1366</td>
<td>210</td>
<td>0.04748</td>
<td>82 - 130</td>
<td>1.375</td>
<td>94.54</td>
<td>69.2</td>
</tr>
<tr>
<td>Atom</td>
<td>Laptop processor</td>
<td>45 nm</td>
<td>24</td>
<td>441</td>
<td>89</td>
<td>0.04443</td>
<td>2 - 13</td>
<td>1.175</td>
<td>1.7 – 11.06</td>
<td>3 - 25</td>
</tr>
<tr>
<td>Intel Core i7</td>
<td>Laptop processor</td>
<td>32 nm</td>
<td>216</td>
<td>1366</td>
<td>208</td>
<td>0.40303</td>
<td>65 - 130</td>
<td>1.375</td>
<td>94.54</td>
<td>69.21</td>
</tr>
<tr>
<td>Atom “Medfield”</td>
<td>Laptop processor</td>
<td>32 nm</td>
<td>64</td>
<td>559</td>
<td>86</td>
<td>0.57245</td>
<td>3.5 - 10</td>
<td>1.21</td>
<td>8.26</td>
<td>14.7</td>
</tr>
<tr>
<td>Intel Core i7 Ivy Bridge E</td>
<td>Laptop processor</td>
<td>22 nm</td>
<td>256</td>
<td>604</td>
<td>161</td>
<td>0.10595</td>
<td>45 - 77</td>
<td>1.4</td>
<td>55</td>
<td>91.05</td>
</tr>
<tr>
<td>Intel Core i7 Haswell</td>
<td>Laptop processor</td>
<td>22 nm</td>
<td>177</td>
<td>2011</td>
<td>238</td>
<td>0.026462</td>
<td>65 - 88</td>
<td>1.4</td>
<td>62.85</td>
<td>31.2</td>
</tr>
<tr>
<td>Intel Core i7 Broadwell-E</td>
<td>Laptop processor</td>
<td>14 nm</td>
<td>246</td>
<td>2011</td>
<td>232</td>
<td>0.031197</td>
<td>140</td>
<td>1.4</td>
<td>100</td>
<td>49.72</td>
</tr>
</tbody>
</table>
References


doi: 10.1109/DATE.2007.364663


