A Revolving Reference Odometer Circuit for BTI-Induced Frequency Fluctuation Measurements under Fast DVFS Transients and Reconfigurable Feed Forward MUX PUF Design

A Thesis
SUBMITTED TO THE FACULTY OF
UNIVERSITY OF MINNESOTA
BY

Saroj Kumar Satapathy

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE ELECTRICAL ENGINEERING

Prof. Chris H. Kim

October 2014

© Saroj Kumar Satapathy 2014

Acknowledgements

I would like to take this opportunity and to thank all the people without whom this thesis could not have been completed.

First and foremost, I would like to express my sincere gratitude to my advisor, Professor Chris H. Kim for his continued guidance and motivation. He constantly shared his technical, writing and presentation skills with me and helped me develop these abilities which will be very useful for my professional career. I could not have had a better mentor for my study.

I would like to thank Professor Keshab Parhi and his group for their help regarding my work on Physical Unclonable Function (PUF). Without his personal guidance, in addition to the support and technical expertise from his team, my work on PUF would not have been successful.

This work would not have been possible without constant encouragement and support of all my colleagues – friends at VLSI Research Lab at U of M. I would like to thank all of my friends for all their help and support.

I would like to thank all my teachers at University of Minnesota whose classes helped me gain knowledge and experience in my field.

Last but not the least; I would like to thank my parents, my past teachers and friends for their guidance, love and support without whom this work would not have been possible.

Dedication

This thesis is dedicated to all my friends here at University of Minnesota, who made my graduate life the most memorable one. This is one of the most fun-filled and happiest periods of my life, which was not possible without all your support and sharing.

I also dedicate this thesis to my parents and family, who understood and supported me on this voyage to make my dreams come true. You have been the best guide of my life.

Abstract

The frequency shift due to fast Bias Temperature Instability (BTI) related fast Dynamic Voltage and Frequency Scaled (DVFS) stress-recovery effects were measured using a high resolution revolving reference silicon odometer. It uses eight fresh/reference ring oscillators (ROSCs), which alternately take measurements three times making a maximum of 24 measurements. Thus the reference ROSCs undergo negligible stress and provide high measurement resolution, low measurement time and fast measurement step coupled with reliable measurements. For the first time, this design provides DVFS frequency shift measurement only in 1µs period after the supply transition. The test chip was implemented in a 65nm process. The frequency shift measurements were observed across different voltage supply, temperature, stress time duration, and supply ramp duration.

Keywords –BTI, stress, recovery, degradation, relaxation, DVFS, transients, revolving reference, odometer, Turbo, high resolution, frequency shift, measurement, supply ramp, supply transition, guard band, on-chip monitor

Table of Contents

List of Figures v

I. Introduction 1

II. Beat Frequency Detection (BFD) Technique 5

III. Revolving Reference Odometer Design 7

IV. Chip Measurement Results 11

V. Basic BTI Measurement 12

VI. BTI Measurement under Voltage Transition 14

VII. Temperature Effect on Voltage Transition BTI Measurement 20

VIII. Long Stress Measurement 23

IX. BTI Measurement under Supply Ramp 27

X. PUF Basics 29

XI. Reconfigurable PUF Design 32

XII. Summary 37

Bibliography 38

List of Figures

Figure 1 Concept of fast DVFS BTI effects (a) V_{DD} and frequency scaling profile (b) V_t shift wrt stress time [4] 2

Figure 2 Beat Frequency Detection (BFD) system 5

Figure 3 Supply voltage and ROSC frequency profile during stress and measurement periods 7

Figure 4 Revolving reference odometer design (a) Block diagram, (b) Supply voltage and ROSC frequency profile 9

Figure 5 65nm test chip die photo with chip summary 11

Figure 6 Measured frequency shift after switching on at 1.2V 12

Figure 7 Measured frequency shift after switching on at 1.4v compared to 0.8v in log-log scale 13

Figure 8 Measured frequency shift at low voltage to high voltage transition....... 14

Figure 9 Measured frequency shift at high voltage to low voltage transition....... 15

Figure 10 Measured frequency shift for series high and low VDD transition 16

Figure 11 Measured frequency shift comparison (a) low to multiple high voltage transition (b) power trend of high voltage degradation.. 17

Figure 12 Measured frequency shift comparison (a) high to multiple low voltage transition (b) log trend of low voltage recovery 18

Figure 13 Measured frequency shift at high voltage to low voltage transition at various temperatures.. 20

Figure 14 Measured frequency shift at high voltage at different temperature..... 21

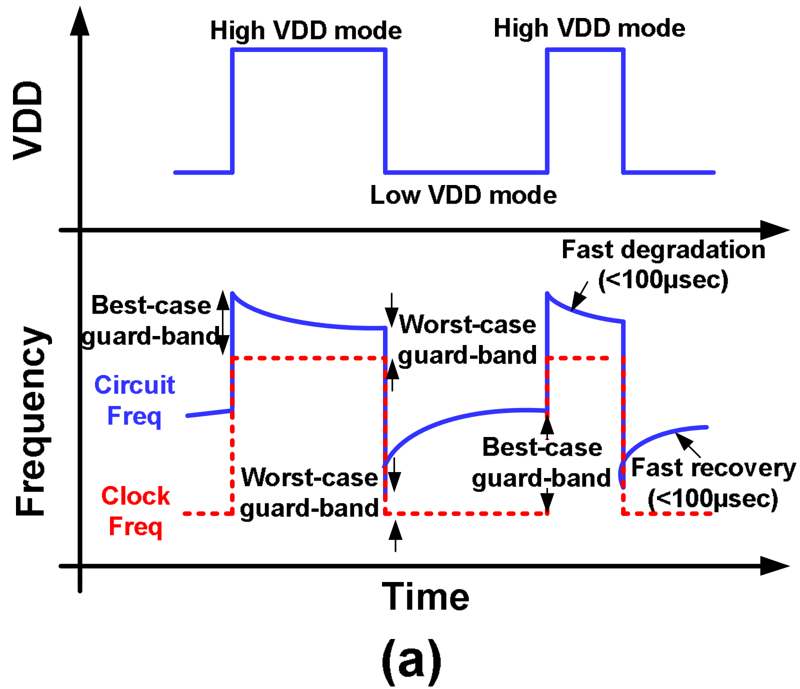
Figure 16 Measured frequency shift from low to high VDD transition for a long stress time 23
Figure 17 Measured frequency shift from high to low VDD transition for a long stress time 24
Figure 18 Measured frequency shift after low voltage transition for a long stress time 25
Figure 19 Measured frequency shift from low to high voltage transition for different supply ramp duration 27
Figure 20 Measured frequency shift from low to high voltage transition for different ramp durations 28
Figure 21 MUX/Arbiter PUF [13] 29
Figure 22 Ring Oscillator PUF 30
Figure 23 Feed forward reconfigurable MUX PUF Circuit 33
Figure 24 Hamming distance distribution of a post layout 32 stage feed forward reconfigurable PUF design with 32 bit challenge-response pair 35
Figure 25 Layout of (a) General and (b) feed forward MUX PUF array in 32nm SOI process 35
Figure 26 PUF with bit error rate (BER) and beat frequency difference (BFD) measurement blocks 36

I. Introduction

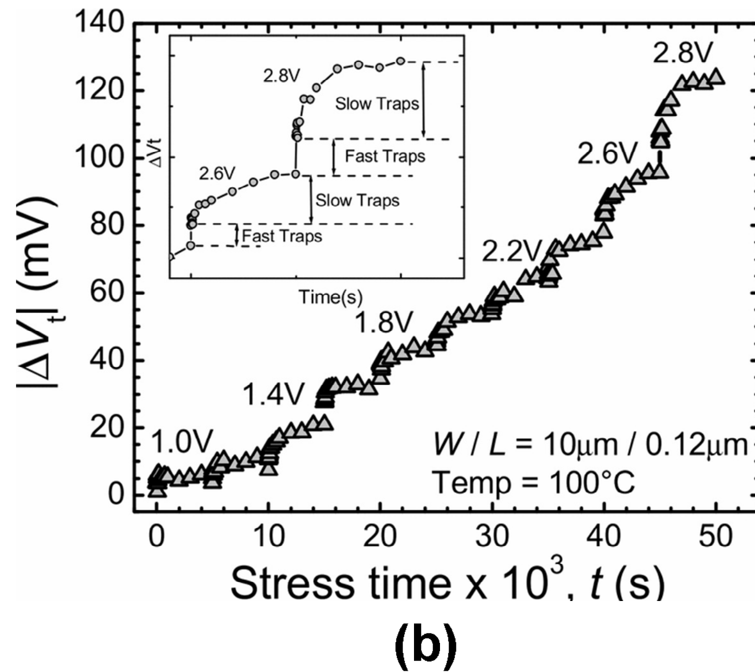
Modern processors employ different power saving techniques like DVFS, turbo/NTV (Near Threshold Voltage) operations and power gating [1]. These techniques employ fast voltage and frequency transients. For example, the new IBM POWER8TM microprocessor uses the integrated voltage regulator module (iVRM) that has micro-regulators (UREGs) featuring sub-ns response [2]. Similarly, the new 22nm Haswell family of processors uses multiple fully integrated voltage regulators (FIVRs), which can ramp voltage supply in sub-microsecond range [3]. The BTI stress and relaxation effects depend on the supply voltage and therefore the reliability profile of these processors differ as compared to single supply voltage systems. Fig. 1 illustrates a typical supply voltage and frequency scaling of a processor, which includes fast BTI degradation and recovery effects. Although fig.1 shows a simple two level turbo and NTV mode transition, real time processors may employ multiple supply voltage transitions.

BTI degradation increases at high supply voltage, so at high VDD mode the inherent circuit delay increases rapidly, reducing the circuit frequency as shown in fig 1(a). When the voltage transition occurs from high VDD mode to low VDD mode, due to the degradation in the previous stage, there is a sudden drop in circuit frequency immediately after the transition. During the low VDD phase,

the circuit frequency undergoes a fast recovery in less than hundreds of



(a)



(b)

Figure 1 Concept of fast DVFS BTI effects (a) V_{DD} and frequency scaling profile (b) V_t shift wrt stress time [4]

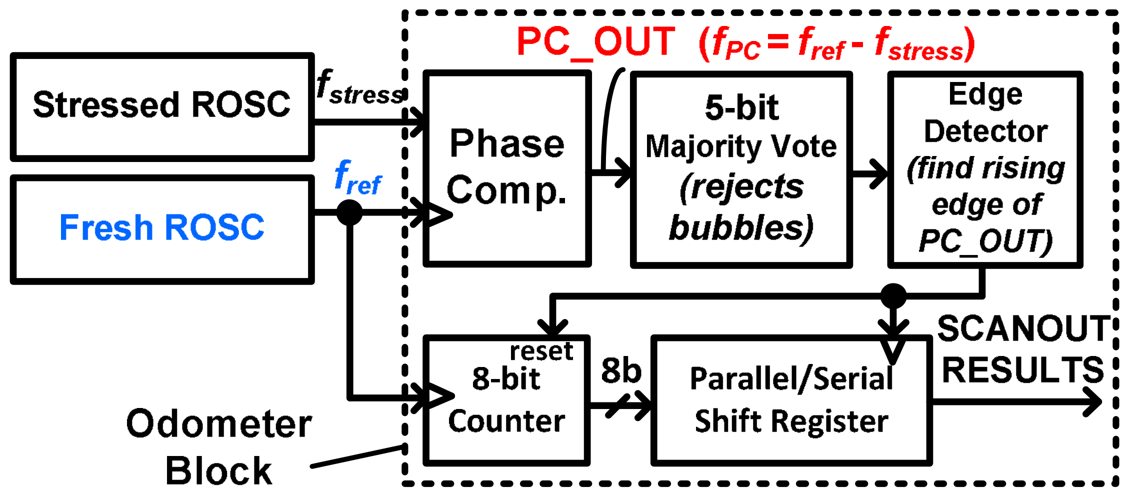
microseconds. In similar process, during NTV to turbo mode transition, the circuit frequency peaks instantaneously and then gradually reduces during the turbo mode. During both these phases, worst-case guard-band occurs right at high VDD to low VDD transition. At this point, the circuit frequency is lowest for the respective modes. Similarly, best case guard-band occurs during low VDD to high VDD transition, where circuit frequency is highest. The fast and slow Vt shift components of BTI is shown in fig 1(b). Experimental data, albeit under accelerated stress conditions, verifies the fast and slow Vt shift components when the supply voltage is increased in steps [4]. It is important to know the amount of instantaneous frequency shifts due to BTI degradation and recovery due to fast DVFS transients. This helps the designers ensure that the clock frequency should not exceed the frequency at worst-case guard-band condition to avoid functional failure of the system. Moreover, knowledge of best-case guard-band can be efficiently utilized for saving energy and processor lifetime [5, 6]. Knowledge of available best-case or worst-case guard-bands also becomes important with device scaling, where the performance and supply voltage margins are shrinking.

There has been no prior work providing silicon measurement of BTI effects induced instantaneous frequency shift in a DVFS environment. [1] is the only work on study of fast DVFS BTI stress and relaxation effects, however that is mostly related to theoretical analysis and modeling. [4] has provided silicon results only for a device level threshold voltage shift, while [7] has provided

frequency shift in a dynamic environment. However, both of them have failed to provide instantaneous BTI effects as their measurement method could capture results only after tens or hundreds of second after the transition. As a result, they are unable to capture the fast degradation and recovery effect that lasts less than 100µs after the transition. This also leads to an inaccurate measurement of worst-case or best-case guard-bands that occurs right after the transition.

This work uses the on-chip beat frequency detection (BFD) [8, 9] based revolving reference odometer, which for the first time measures BTI induced fast degradation and recovery frequency shift in a µs duration after the supply transition in a fast DVFS environment. The use of on-chip BFD based revolving reference odometer also ensures shorter measurement time, reduced test structure area, shorter test times, simpler test set-up and accurate result (in the resolution of 0.01%) in frequency difference readings. The remainder of the paper is organized as follows. Section II introduces the on-chip BFD concept and describes the chip design. Section III discusses the measurement results. Section IV summarizes the advantages and short-comings of this measurement technique.

II. Beat Frequency Detection (BFD) Technique



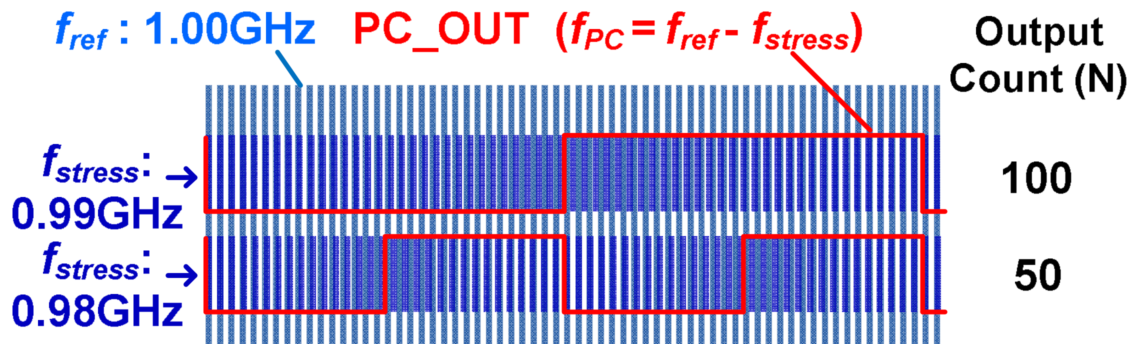


Figure 2 Beat Frequency Detection (BFD) system

The revolving reference odometer design is based on the beat frequency detection technique [8, 9]. Fig 2 shows the block diagram, where two identical ring oscillator (ROSC), one stress and one fresh, produce near identical frequencies. A flip flop used as phase comparator measures the frequency difference, PC_OUT, also known as beat frequency. The final output count

stored in the shift register corresponds to number of fresh ROSC periods within a single beat signal period. The beat frequency detection scheme works well even if the frequencies are closer to each other. For instance, it can measure a frequency difference as close as 0.01%, which corresponds to an output count change from 100 to 99. The high resolution measurement achieves a sub-ps frequency difference measurement resolution with sub-μs measurement time.

III. Revolving Reference Odometer Design

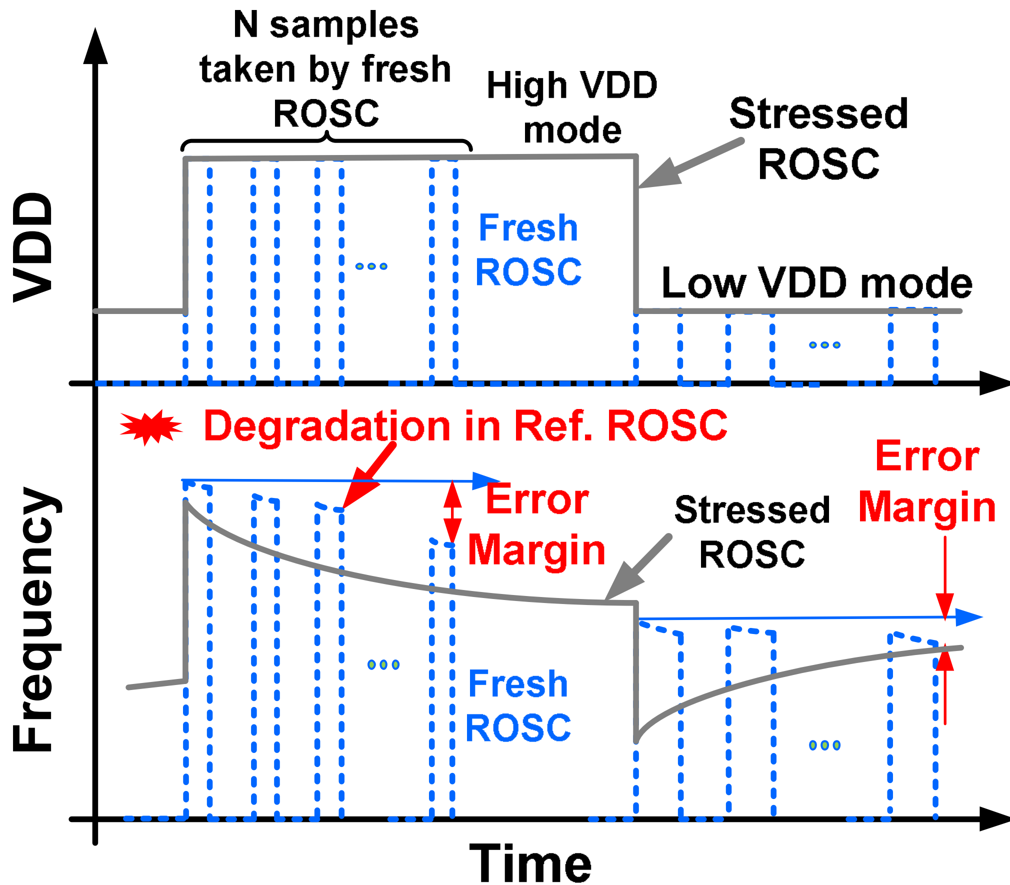


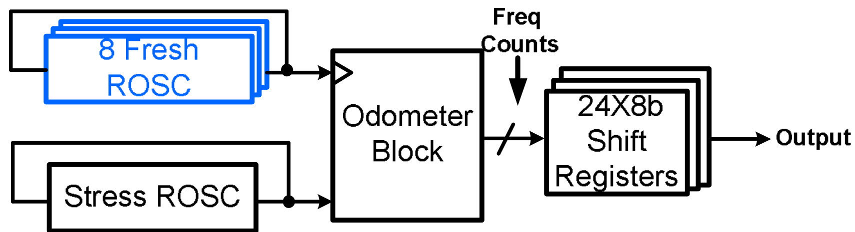
Figure 3 Supply voltage and ROSC frequency profile during stress and measurement periods

Using the BFD technique, the stressed ROSC undergoes the high and low supply voltage transition. Generally during short measurement time, both stressed ROSC and fresh ROSC are both supplied nominal voltage. This is

required to cancel any voltage variation in the measurement. After measurement, stressed ROSC is quickly brought back to its original high or low supply mode, while fresh ROSC can be turned off as before. However, due to the sensitive frequency change associated with a fast DVFS transition, it introduces error in measurement as stressed ROSC can undergo unwanted recovery or stress when measured at nominal voltage. Therefore, we decided to supply the fresh ROSC high or low supply voltage, while the stress ROSC is untouched as shown in top waveform of fig 3. Though a disadvantage associated with this method is that the fresh ROSC undergoes degradation mainly during high voltage supply, as shown in the bottom waveform of fig. 3. This introduces an error margin in the measurement.

To overcome this disadvantage, this design introduces two innovative design techniques. The first design technique uses eight fresh ROSC instead of just one, as shown in fig 4(a). These fresh ROSCs are fired sequentially one after another during measurement for three cycles, as shown in fig 4(b), producing a maximum of 24 measurement samples before the data is scanned out. So, a particular fresh ROSC goes through longer recovery phase before the other seven ROSCs measures and cycles back. This introduces very low error margin in measurement, which can be neglected for all practical purposes. The measurement shows that in worst case measurement, an individual ROSC is on for only around 1% of the total time at a high VDD supply of 1.4V. Although for a typical measurement, this time fraction reduces to 0.0003%, which can be

neglected for all practical purpose. Moreover, if the supply voltage is increased, the measurement time is reduced due to increase in ROSCs frequency. This reduces the time the fresh ROSCs needs to be ON for measurement, thus making the error margin negligible.



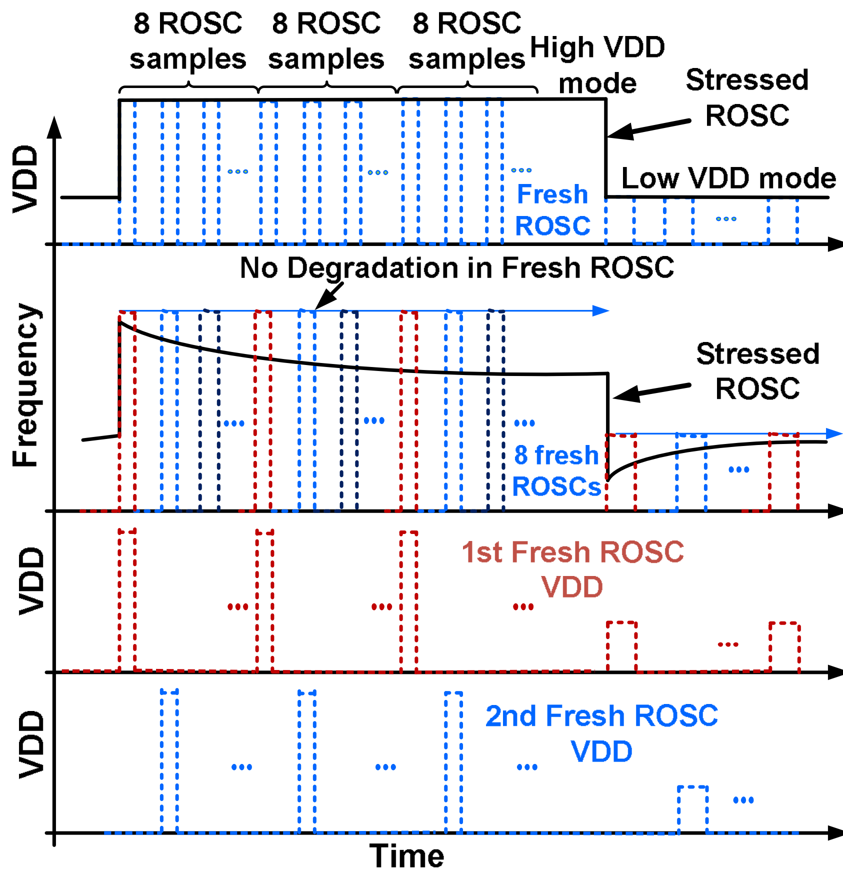
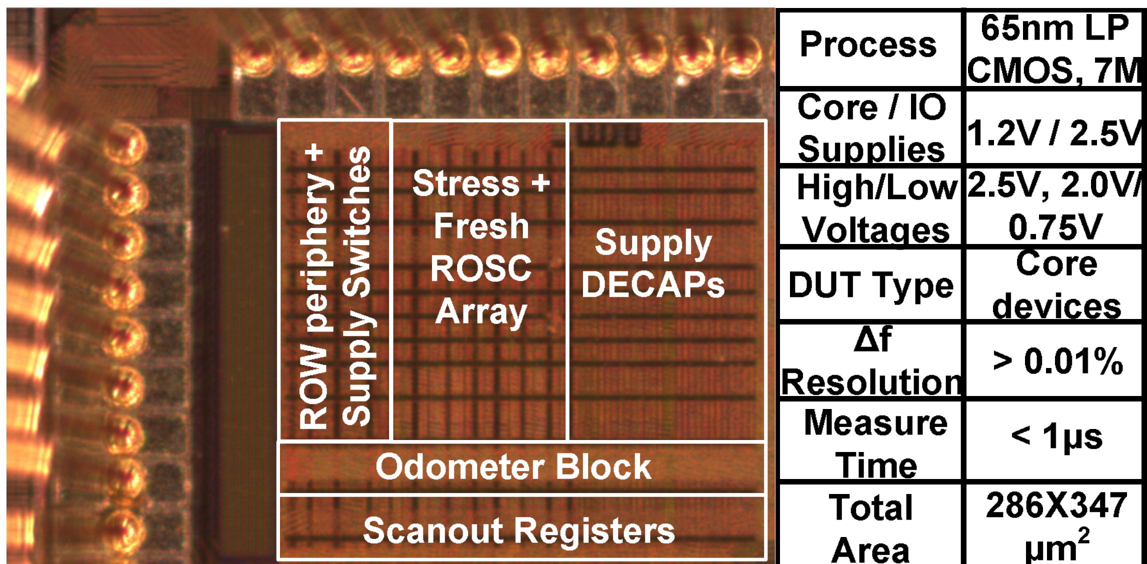


Figure 4 Revolving reference odometer design (a) Block diagram, (b) Supply voltage and ROSC frequency profile

The second design technique is to assist fast on-chip sampling of frequency shift data, we have 24 8-bit parallel-serial scan-out shift registers. This is an improvement over previous BFD designs, which used just one 8-bit parallel-serial shift registers. This ensures that the measurements are not interrupted in between to scan out the data before the next measurement. So, all the 24 measurements are done on-the-fly with minimum time gap between the measurements.

IV. Chip Measurement Results

A test chip was implemented in 65nm process (Fig. 5). We measured the frequency shift in DVFS environment under different voltage and temperature condition. We also measured the shift under long stress time of around 100,000 seconds and under various supply voltage ramp duration during transition. The measurements are described in the next sections.



Process	65nm LP CMOS, 7M
Core / IO Supplies	1.2V / 2.5V
High/Low Voltages	2.5V, 2.0V/ 0.75V
DUT Type	Core devices
Δf Resolution	> 0.01%
Measure Time	< 1μs
Total Area	286X347 μm^2

Figure 5 65nm test chip die photo with chip summary

V. Basic BTI Measurement

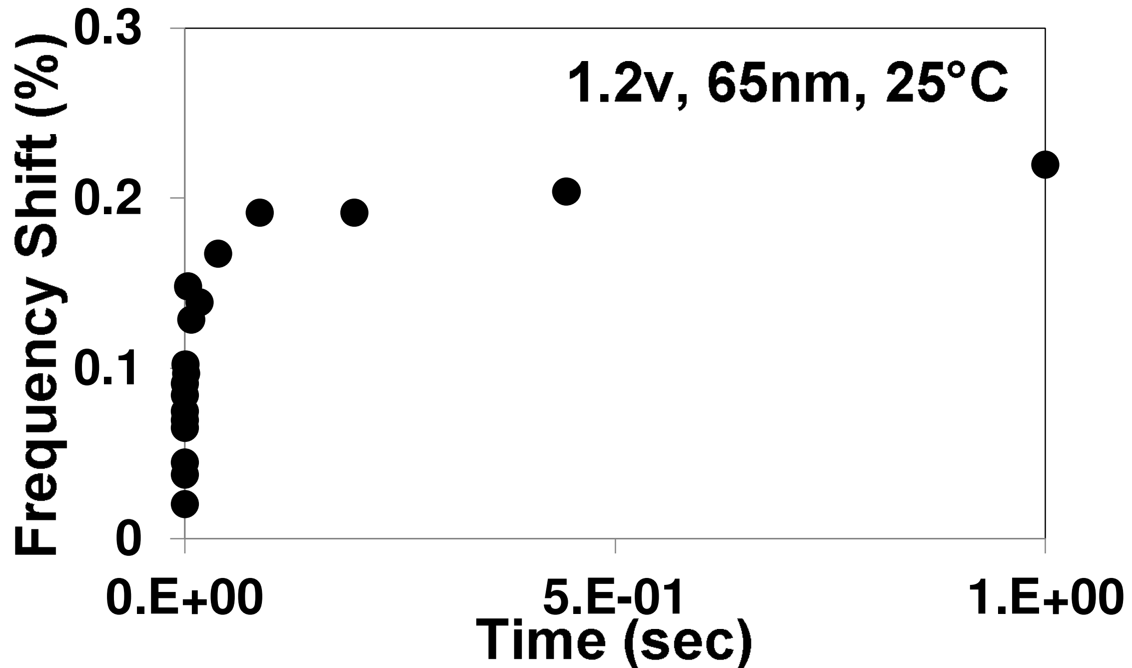


Figure 6 Measured frequency shift after switching on at 1.2V

When any circuit is switched on, it undergoes BTI degradation irrespective of high, low or nominal voltage. Fig 6 shows the measured frequency shift when the chip is powered on at nominal voltage of 1.2V in a linear scale. The first measurement was taken at as early as 1µs time after power was switched on. It measured the result until 1 second. Fig 7 shows the same measurement as compared to a low voltage of 0.8V and high voltage of 1.4V in a log-log scale. Both the measurement shows a clear power trend of BTI degradation.

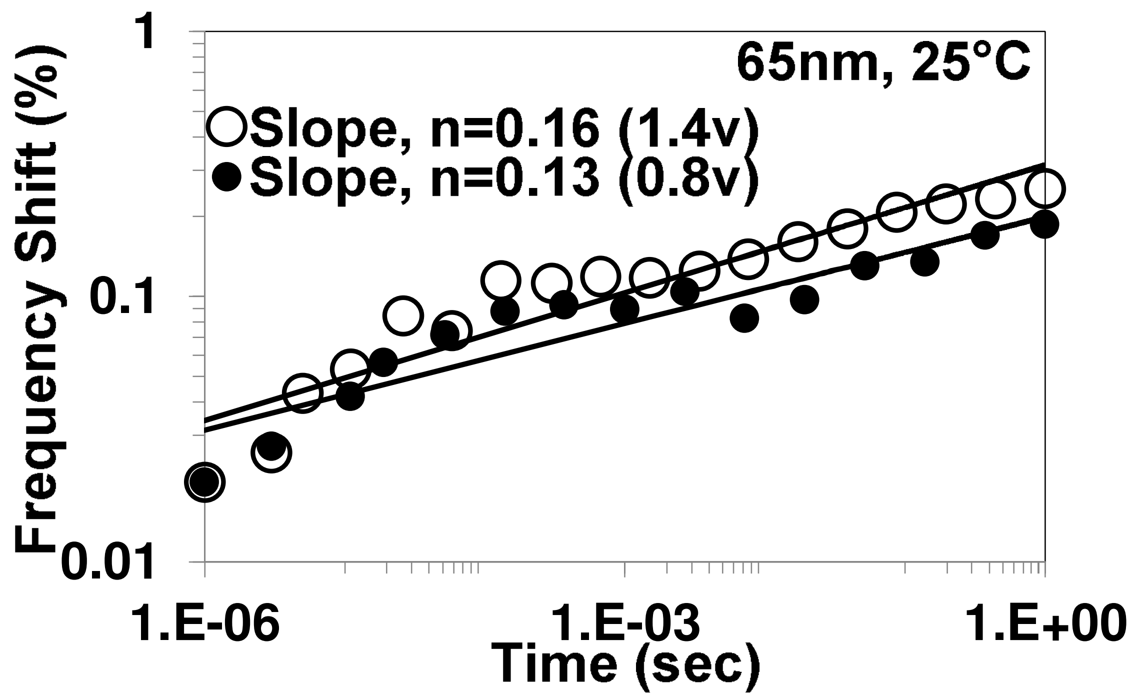


Figure 7 Measured frequency shift after switching on at 1.4v compared to 0.8v in log-log scale

VI. BTI Measurement under Voltage Transition

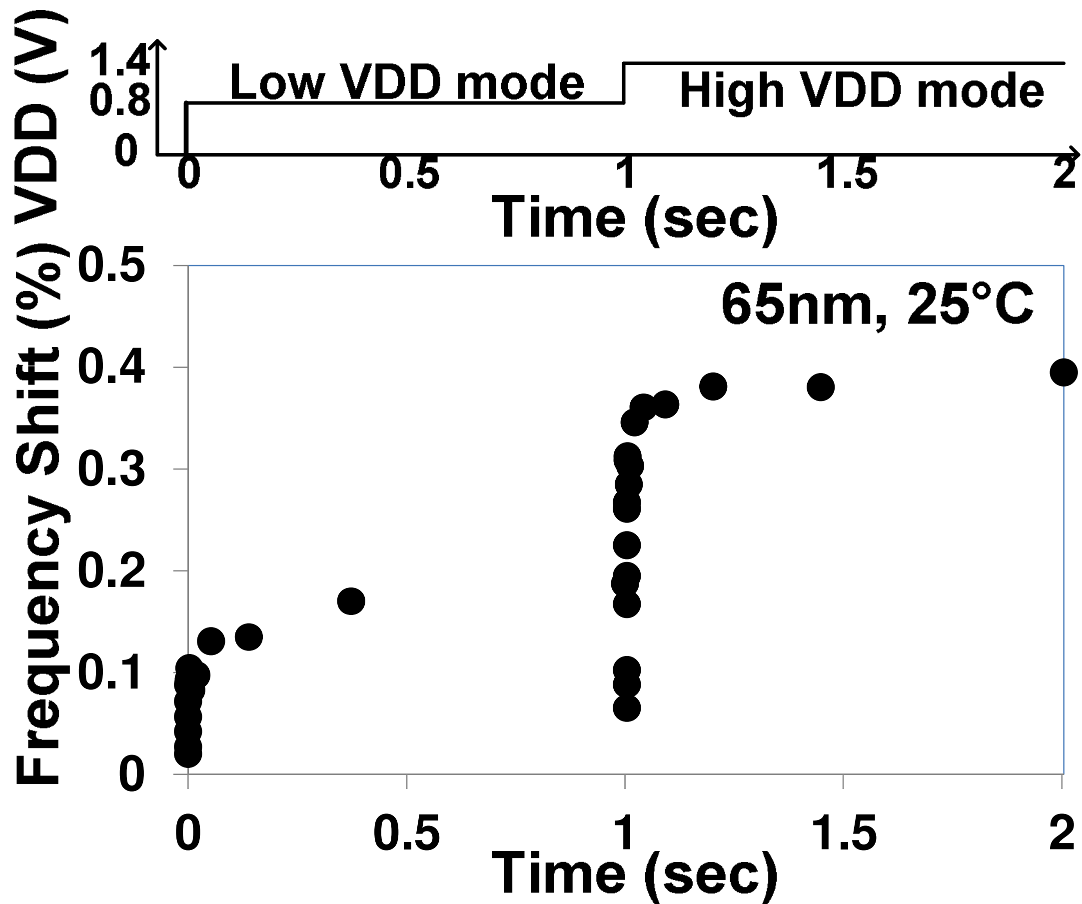


Figure 8 Measured frequency shift at low voltage to high voltage transition

When the supply voltage goes low to high (Fig 8), the frequency shift drops to an initial low value. This can be explained by following equation for frequency shift [1]

$$\frac{\Delta f}{f} = \frac{\Delta V_T}{VDD - V_T}$$

Here, V_T is the threshold voltage and VDD is the voltage supply. So, in a low to high transition of supply voltage, since the VT or ∆VT are same during the time of transition, a steep drop was seen in frequency shift as in fig 8.

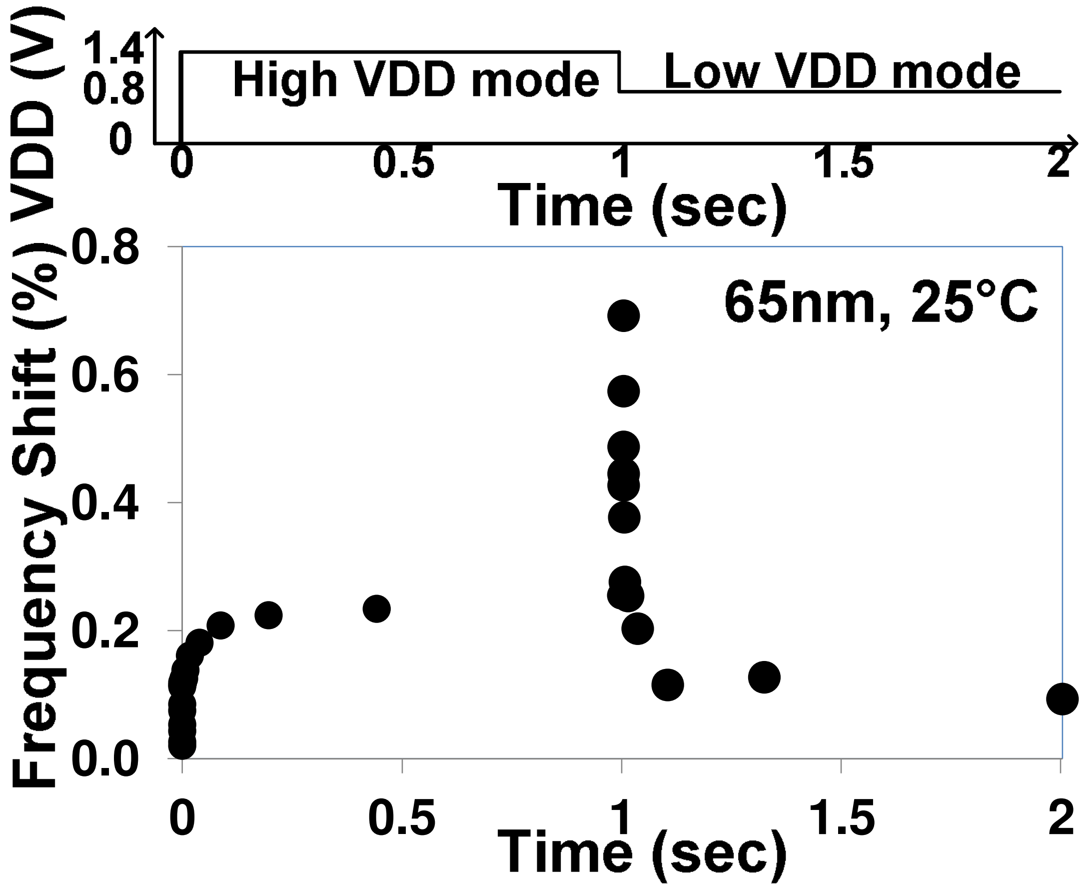


Figure 9 Measured frequency shift at high voltage to low voltage transition

Similarly, in fig 9, a steep jump was observed in the frequency shift during the transition. After that the circuit degrades in the low to high voltage with frequency shift increasing and recovers in the high to low voltage supply transition. The recovery undergoes a logarithmic trend for our measurement.

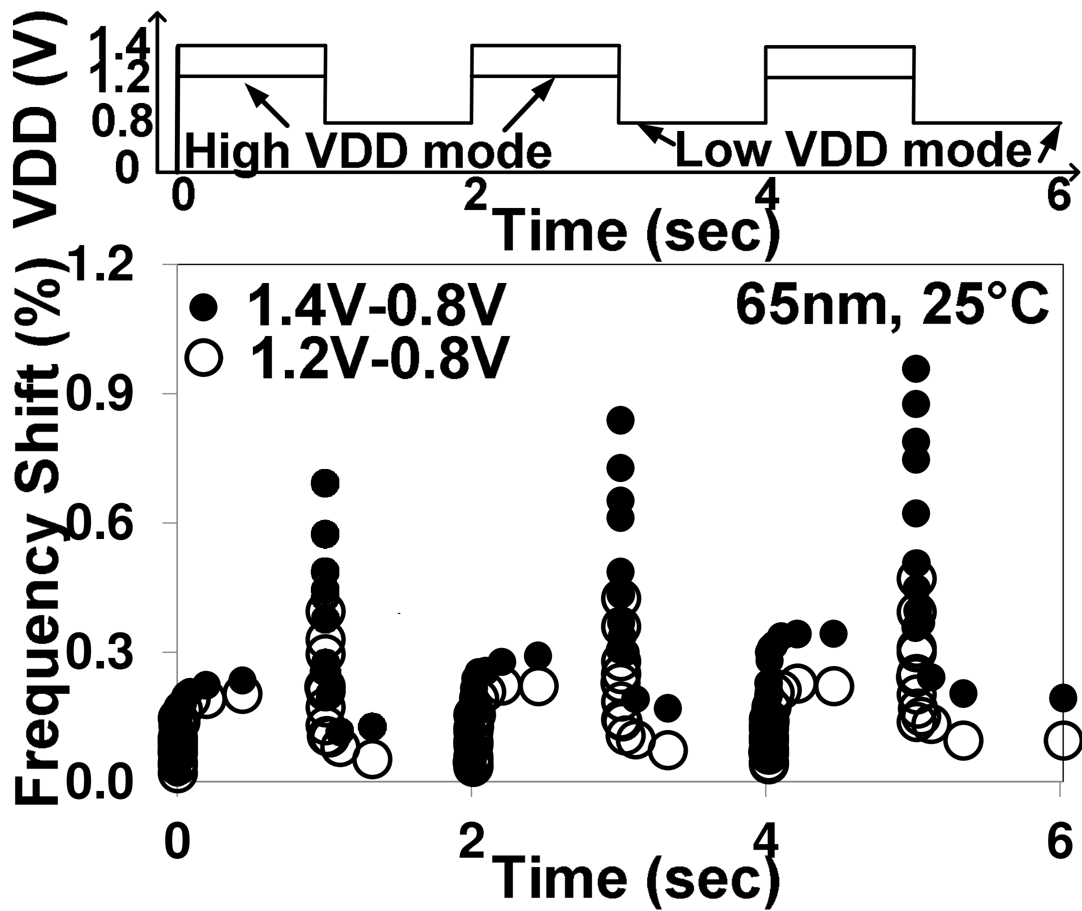


Figure 10 Measured frequency shift for series high and low VDD transition

Fig 10 contrasts series of six transitions between 1.4V/0.8V and 1.2V/0.8V at durations of 1 second each. The frequency shifts were observed to be higher for 1.4V/0.8V pair as the devices undergo more degradation and recovery at extreme voltages as compared to 1.2V/0.8V transitions.

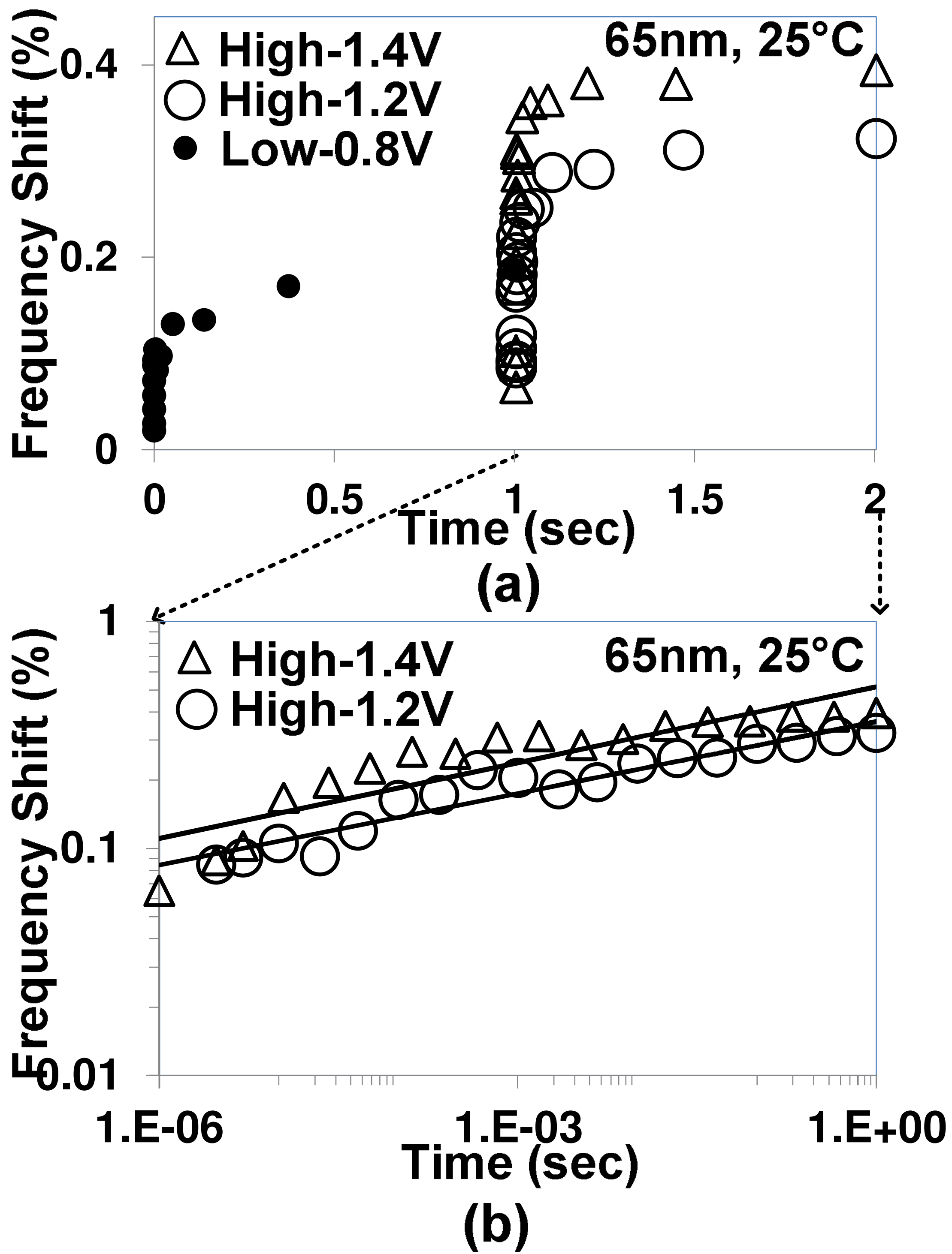


Figure 11 Measured frequency shift comparison (a) low to multiple high voltage transition (b) power trend of high voltage degradation

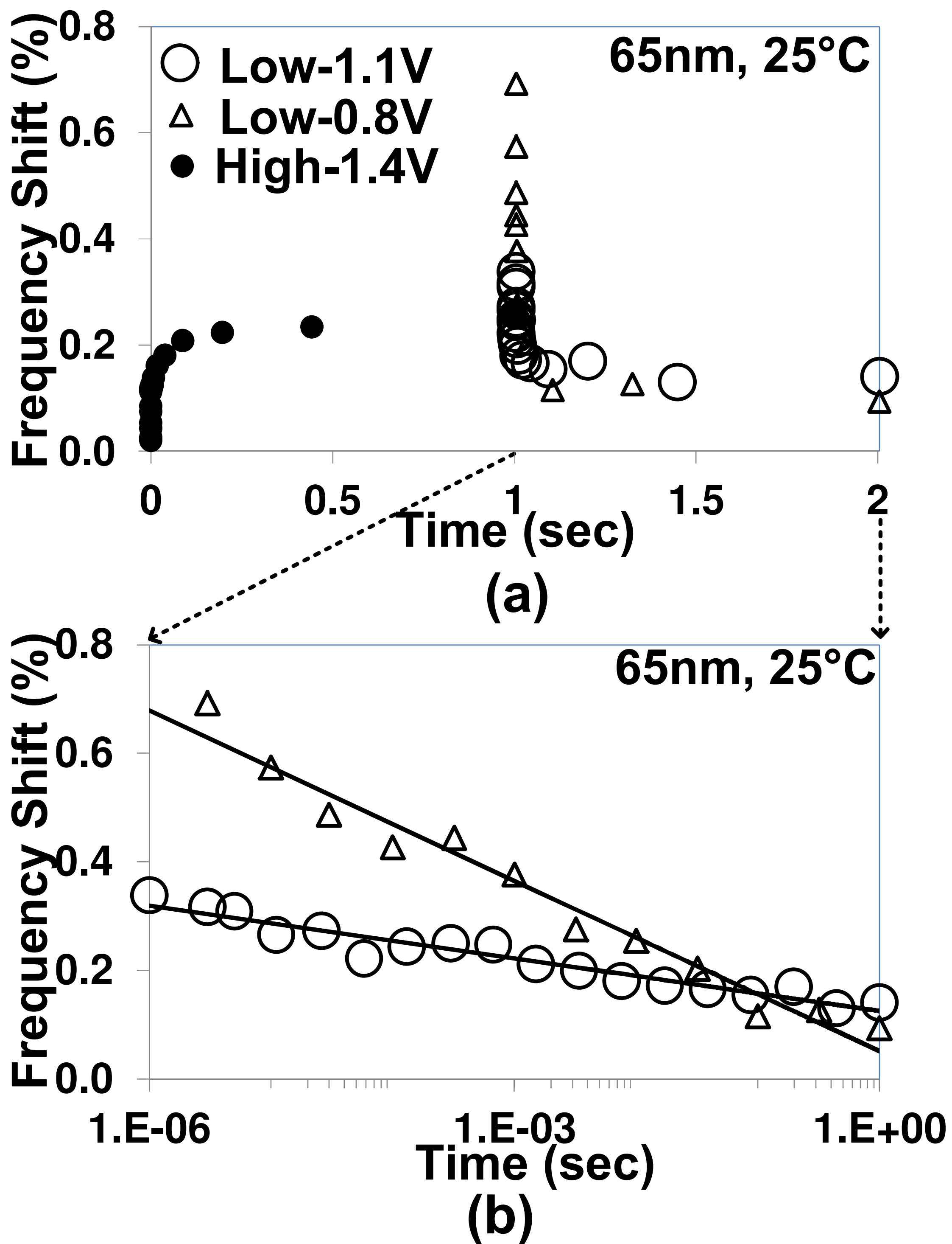


Figure 12 Measured frequency shift comparison (a) high to multiple low voltage transition (b) log trend of low voltage recovery

A comparison between low to high supply transition was shown in fig 11(a), when supply is changed from 0.8v to 1.2V/1.4V. The frequency shift drop was maximum in 1.4V and decreases gradually for 1.2V. This confirms to the equation (1). However, at the end of 1 sec from the transition, 1.4V undergoes greater degradation as compared to 1.2V, respectively. It proves that higher voltage has higher degradation. Fig 11(b) shows the power trend of the degradation at higher VDD mode.

Similarly, fig 12 shows a comparison between multiple low voltage after transition from a 1.4V high supply voltage. Confirming equation (1), highest frequency shift jump was observed for 0.8V and gradually decreases as the supply voltage increases. Fig 12(b) shows a logarithmic recovery process after high to low voltage transition.

VII. Temperature Effect on Voltage Transition BTI Measurement

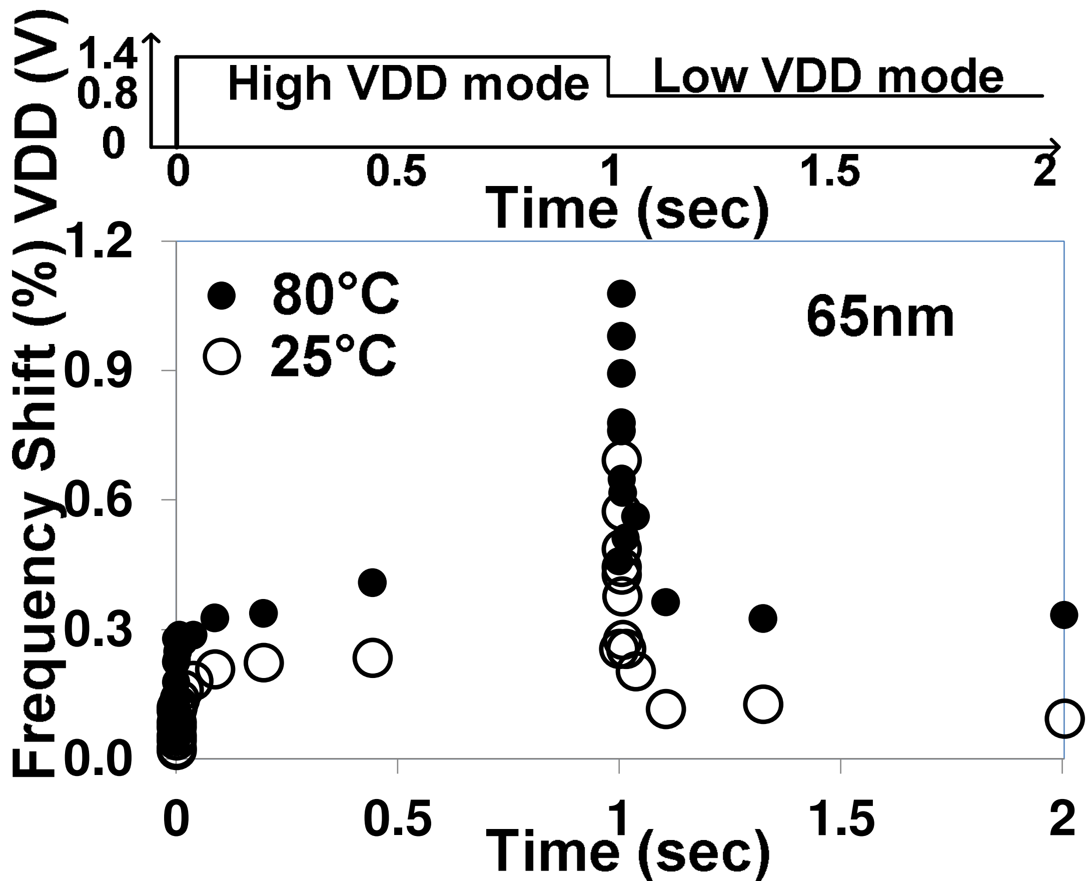


Figure 13 Measured frequency shift at high voltage to low voltage transition at various temperatures

BTI is more sensitive to temperature i.e. the frequency shift increases at higher temperature. Fig 13 shows the temperature effect for a high voltage to low voltage transition at 80℃. Although the shape of the frequency shift follows the same trend, the amount of frequency shift increases when compared with fig 8 at

25℃. A comparison of the degradation at different temperature is shown in fig 14 and the contrast between the recovery is shown in fig 15.

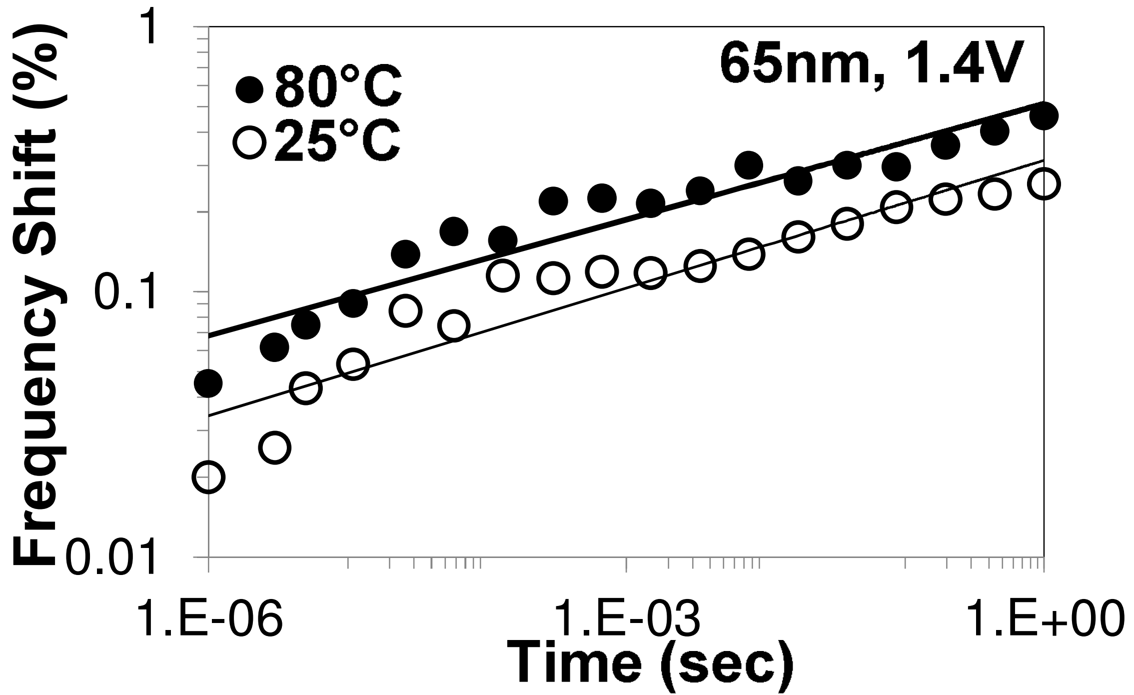
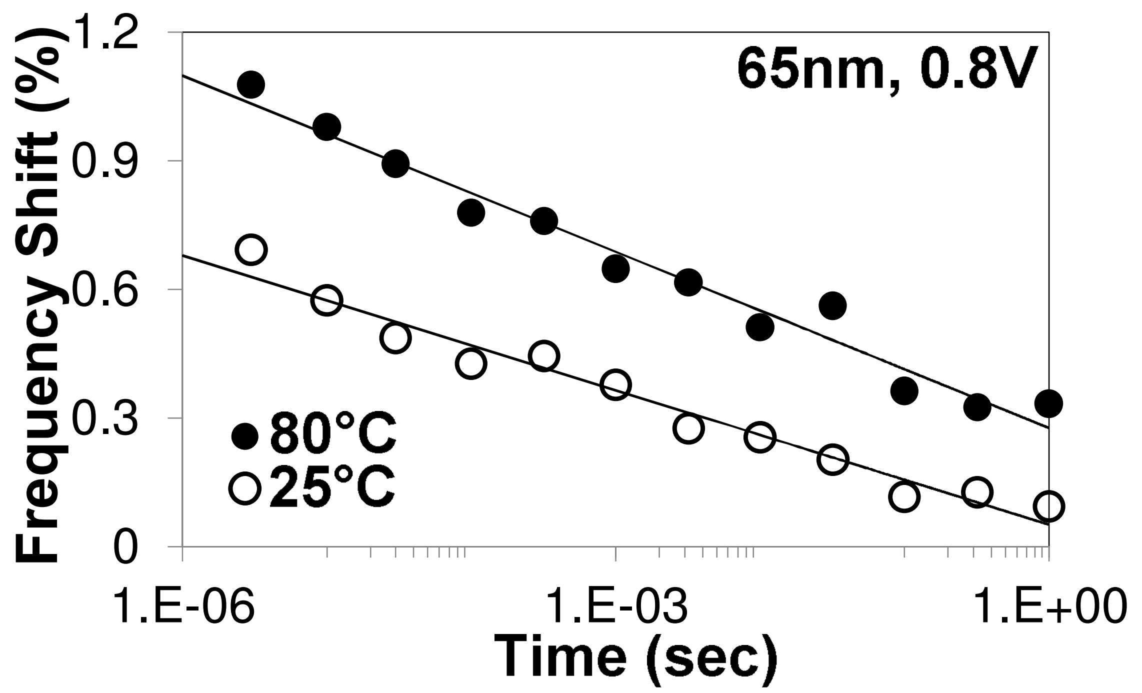


Figure 14 Measured frequency shift at high voltage at different temperature

Fig 14 shows that at both room temperature and higher temperature, the shape of the curve remains the same and power trend is observed. However, the amount of shift at higher temperature is around twice of that in room temperature. A similar conclusion can be drawn through fig 15, where we can observe a similar logarithmic trend in recovery at both temperatures, while BTI has higher sensitivity at high temperature resulting in higher frequency shift.


65nm, 0.8V
80°C
25°C
Frequency Shift (%)
Time (sec)
1.2
0.9
0.6
0.3
0
1.E-06
1.E-03
1.E+00

VIII. Long Stress Measurement

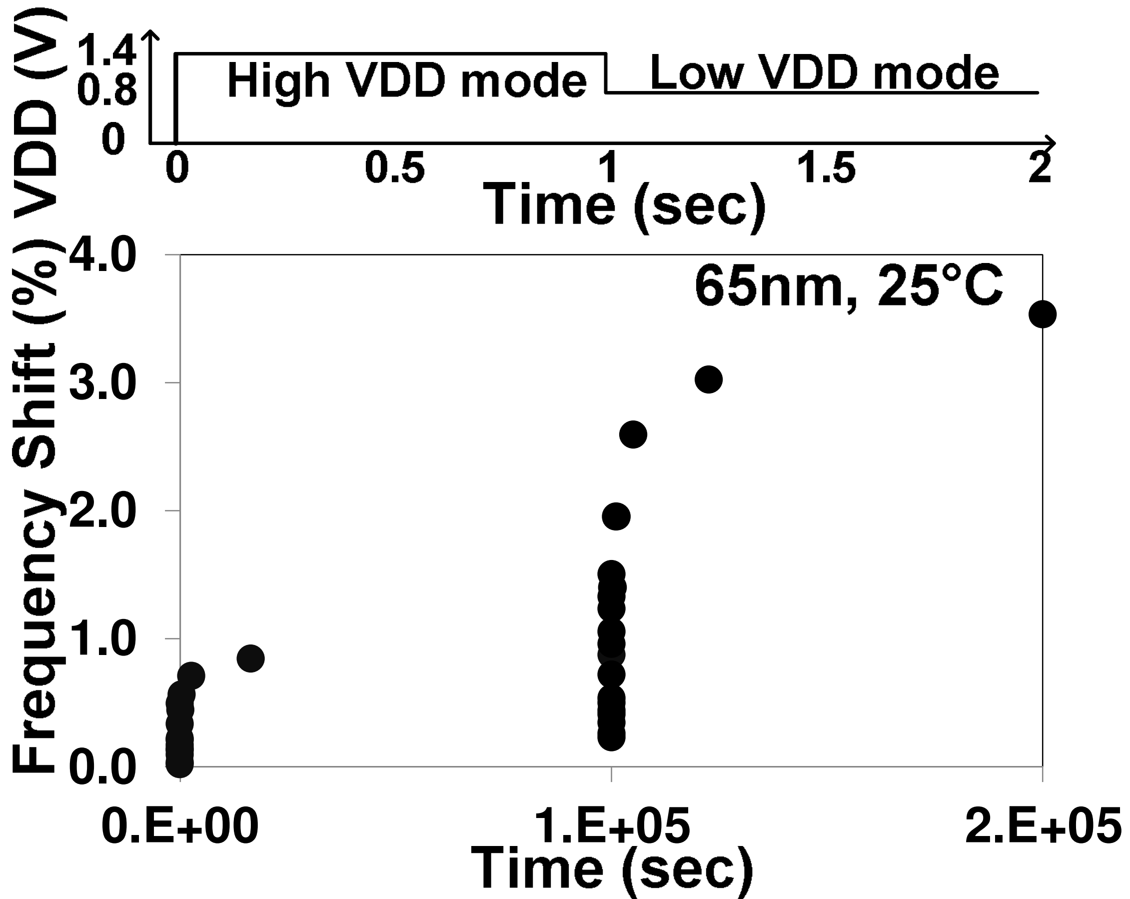


Figure 16 Measured frequency shift from low to high VDD transition for a long stress time

The test design was subjected to a long stress of around 100,000 seconds per high/low VDD cycle to observe the extreme frequency shift after the long stress cycle. Fig 16 presents the low supply (0.8v) to high supply (1.4v) transition of the long measurement. The BTI degradation follows the same power trend, but this time the amount of degradation is very high. At the end of low supply

transition the frequency shift was observed near 1%. After a strong dip at the transition to higher VDD of 1.4v, again the BTI degradation frequency shift reaches to around 3.5%. As compared to a 1 sec stress where the frequency shift stayed below 0.5%, this is a strong degradation owing to the long stress cycle. The frequency shift will be even more if the time duration for stress is higher.

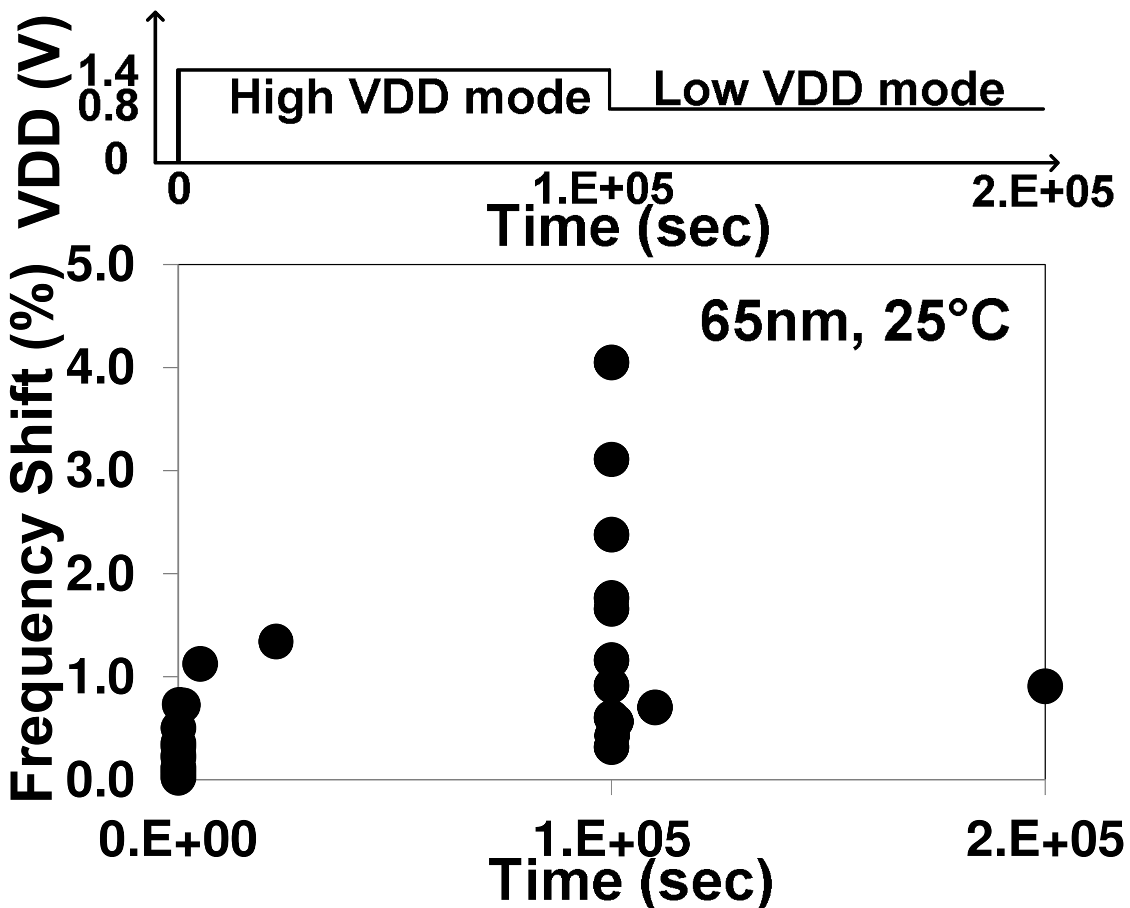


Figure 17 Measured frequency shift from high to low VDD transition for a long stress time

Similarly, fig 17 represents the high to low voltage transition measurement of 100,000 seconds of stress per cycle. Here the frequency shift reaches to

around 4%, immediately after the devices transitioned from a stress voltage of 1.4v to a low voltage of 0.8v. This is owing to the huge degradation undergone during the 100,000 seconds of 1.4v stress in the first cycle. The worst frequency shift was observed near to 2% during the end of this duration, before the transition.

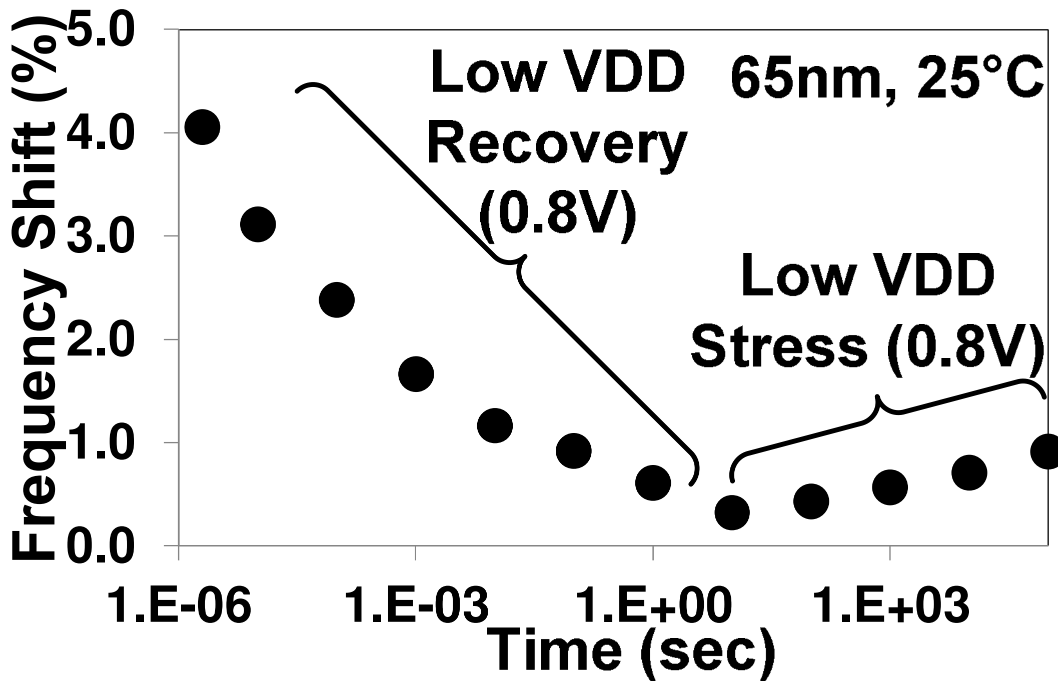


Figure 18 Measured frequency shift after low voltage transition for a long stress time

Another phenomenon that was observed after the transition is the gradual recovery and degradation at the end of low voltage cycle. Fig 18 clearly demarcates the measurement point, where the measurement underwent a logarithmic recovery after the high voltage stress cycle. However, after around 10sec, the degradation due to 0.8v dominated over the recovery due to the

previous phase and the devices started to show a BTI degradation dominated frequency shift. [1] discussed a similar concept of super-position model, where it proposed the overall effect during the recovery phase is the sum of individual recovery component due to the previous stress cycle and the degradation component due to the low voltage stress that the devices is undergoing. In theory, our measurement results confirms with the super-position model, both of which individual effects can be seen during the long stress measurement.

IX. BTI Measurement under Supply Ramp

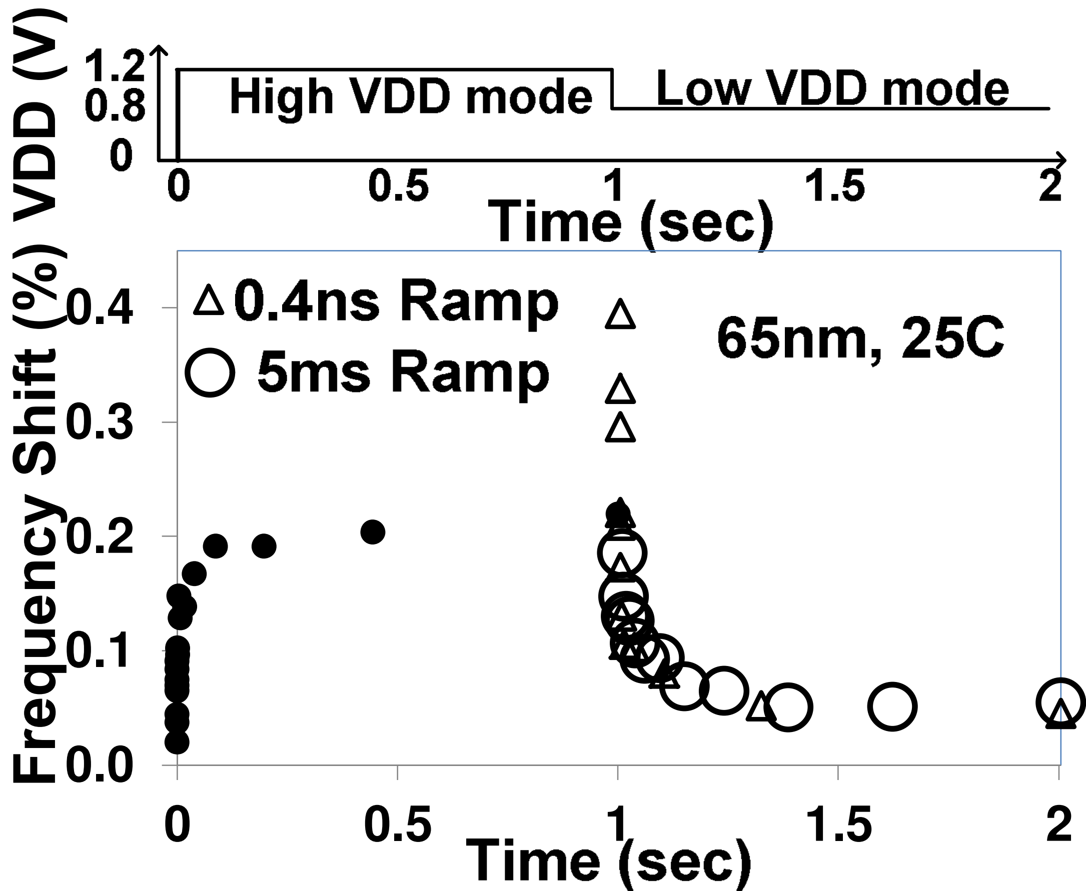


Figure 19 Measured frequency shift from low to high voltage transition for different supply ramp duration

In all the previous measurements, the test chip was subjected to an on-chip supply voltage ramp of around 0.4ns. Effect of a long supply ramp time was also measured. Fig 19 compares the high to low supply transition with a 0.4ns supply ramp to a 5ms supply ramp. We can see that the supply ramp dilutes the

frequency shift effect that was seen in a lower ramp time. In this case, the highest frequency shift observed was even lower than observed during the high VDD mode of 1.2v. Fig 20 shows a similar effect for a low to high power supply transition, where the frequency shift dip observed during 5ms ramp time was lower than that of observed during 0.4ns ramp time.

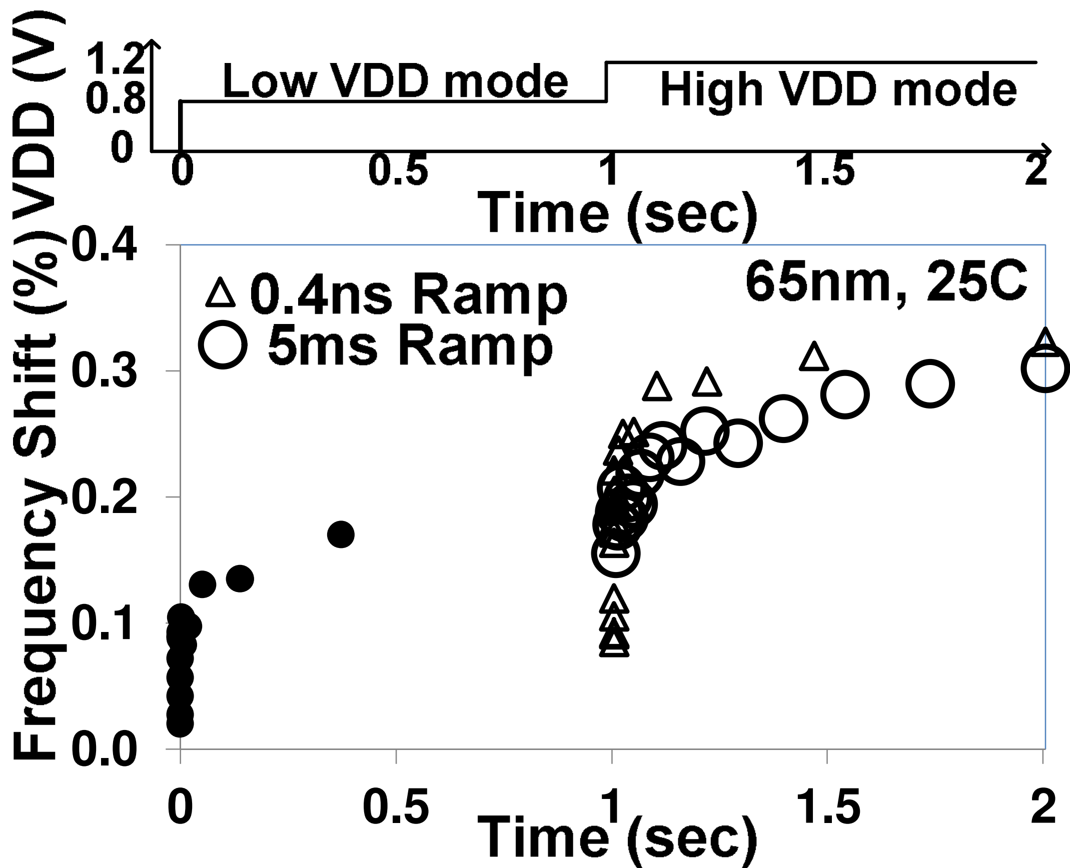


Figure 20 Measured frequency shift from low to high voltage transition for different ramp durations

X. PUF Basics

PUFs exploit unique and random circuit characteristics resulting due to inherent process variation, and are nearly impossible to predict, clone or duplicate. PUFs were invented in 1992 by Naccache and Frémanteau. When a PUF design is provided with an input (or challenge), the output (or response) should satisfy the following properties: Unique output depending on die variation, Random i.e. difficult/impossible to model the response and Reliable i.e. consistent across environmental variations, aging [10]. Our main area of work is on PUFs that can be designed on Silicon [11]. Some of the silicon PUF includes the SRAM PUF [12], which uses the initial state of SRAMs to extract secret keys. Some other PUFs are the MUX PUF [10] and the Ring Oscillator (RO) PUF [10] that utilizes the challenge-response characteristics rather than storing the secret keys like SRAM PUF. Fig. 21 and fig. 22 describes the circuit of a MUX PUF and RO PUF, respectively.

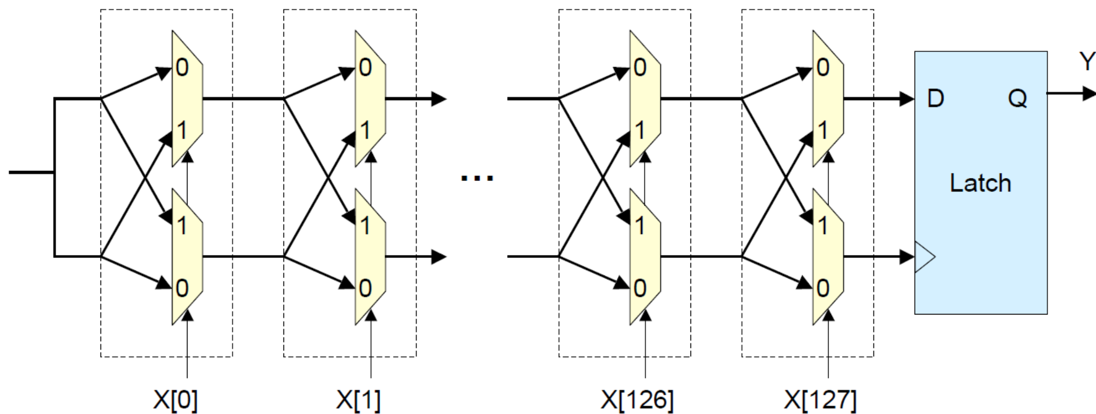


Figure 21 MUX/Arbiter PUF [13]

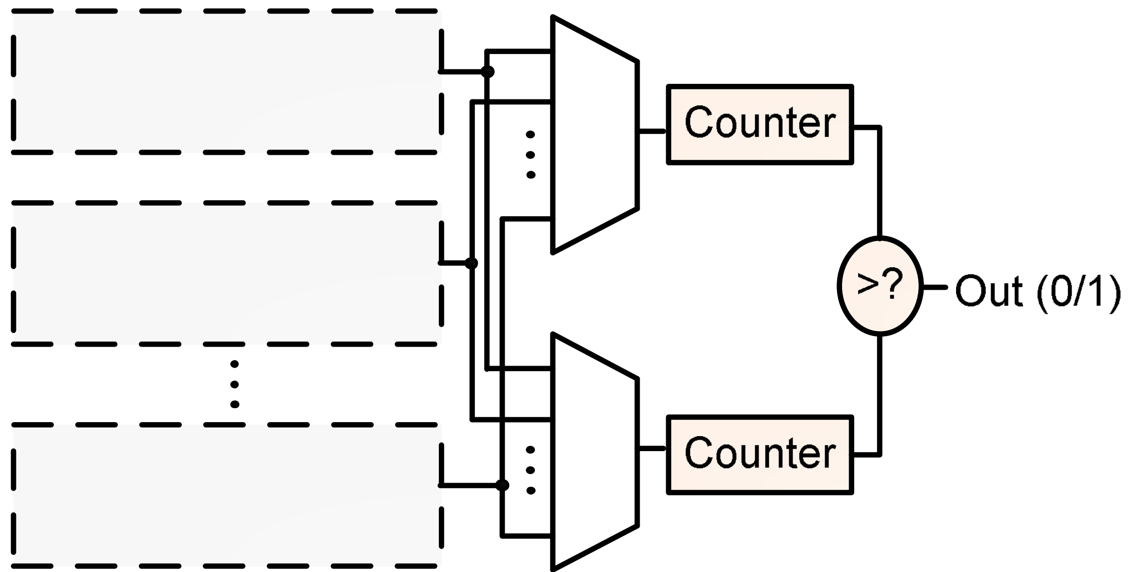


Figure 22 Ring Oscillator PUF

A MUX or an Arbiter PUF has two identical delay paths. However, due to manufacturing variations they have slightly different delays. The paths connect to an arbiter that makes decision as to which path is faster. This decides the response of the PUF. On the other hand, RO PUFs consists of multiple identical ROs and generates a random bit by comparing frequencies (measured by counters) of a selected pair of ROs. So, RO PUF is similar to a MUX PUF [10]. MUX PUF designs are simple and easier to attack without obfuscation, while the RO PUF is slower, larger and consumes more power. So, the MUX PUF is appropriate for resource constrained platform, while RO PUFs are better for FPGAs [13]. Right now we are exploring MUX PUF for its simple design and efficient implementation on chip, but we are also exploring other advanced PUF for future work.

There has been a lot of work in PUF in past. A Silicon PUF inter-die variation provides it unique output characteristic and intra-die variation provides it reliable output characteristic. So, there is a need to analyze these data on the die. However most of the previous works are based on FPGAs or older technologies. Some of the recent work has been done on 90nm standard CMOS process or FPGAs [14, 15]. So, there is a need to explore the PUF characteristics on the current process. Also there is a requirement to understand how the variation will affect the PUF properties, especially the intra-die reliability with extreme variation in PVT. This will help in detecting the unreliable challenges and response pairs that can be discarded to make the PUF secure and reliable.

XI. Reconfigurable PUF Design

Our work addresses mainly three innovative techniques for the PUF design: use of reconfigurable MUX PUF in an advanced 32nm SOI process, use of high resolution on-chip BFD system to quantify the unreliability of the two delay path of the MUX PUF by calculating frequency difference of the two delay paths and use of on-chip Bit Error Rate (BER) measurement to calculate the bit error rate for reliability calculation at different PVT.

Our design will be fabricated on silicon using advanced 32nm SOI process. This will help analyze the post-layout and on silicon variation. For example, while designing a MUX arbiter PUF, it is very essential for the two delay paths to be symmetric. Even a slightly biased SR latch arbiter, where the NAND gate inputs were interchanged, it gave us a peak hamming distance at 20% instead of 50% through Monte-Carlo schematic simulations. So, it is essential to analyze layout techniques for symmetrical design and how it results in the uniqueness in the response among different chips. At the same time, while designing general MUX PUF, we will also analyze the feed forward PUF in the same die. A feed forward PUF as shown in the fig. 23 is a different configuration of general PUF that uses the racing result of an intermediate stage as the select signal for a block of MUXs in a later stage depending on the select bit [16]. Due to its non-linearity, it is suggested that it increases randomness of the PUF. In our proposed work, we will re-use the general PUF to design the feed forward PUF on chip, so that we can compare and quantify the advantage over general

MUX PUF. There are other kinds of MUX PUF configuration available that also we are going to explore through a unified reconfigurable PUF [16]. This PUF can be reconfigured depending on the select bit to work as different configurations or a combination of configurations at a time. This will provide us useful hardware comparison data and thereby select the best configuration for different application.

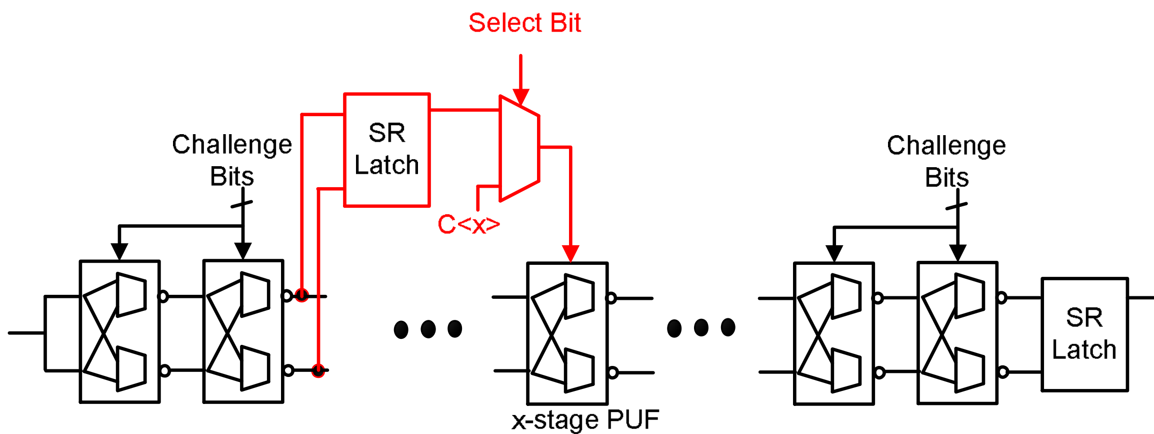


Figure 23 Feed forward reconfigurable MUX PUF Circuit

Also for the first time the proposed work provides on-chip measurement circuit to quantify these variations using our BFD silicon odometer that monitors high resolution frequency shift [8, 9]. The basic technique is shown in the figure 2. The proposed design can capture a frequency shift more than 0.01%. The high resolution offered by this device will help capturing even the sensitive device reliability degradation effects such as BTI effects. If this frequency difference is too low for the response to be unreliable, we can either discard it or process it to correct the output. This will improve the reliability of the PUF on-chip by monitoring the intra-die variation.

Also for a PUF to be reliable, it needs to be tested on silicon under extreme PVT condition to be industry ready. For the first time, our work will analyze the reliability by calculating the bit error rate (BER) through on-chip BER measurement circuit. The circuit will analyze the result under different PVT condition. For the BER circuit to be more accurate, it has the feature to analyze outputs on either case of the first delay path being faster or slower than others. That will help in deciding to measure only the unreliable bits that will be less in number and therefore the counter to provide an accurate BER number. A statistical analysis will provide useful information with respect to intra-die variation at different PVT conditions and even capture the sensitive effect of device reliability degradations. On a different directions, our work, with the help of on-chip BER measurement circuit, will also help us to analyze NTV based PUF designs and how it helps us getting unique responses when inter-die variation will increase under low supply voltage condition. It will also give us some inputs on how random are the device reliability degradations and how it can be used for PUF designs based on random variations due to device reliability.

Fig. 24 shows Hamming distance distribution (inter chip) of a post-layout 32 stage feed-forward reconfigurable MUX PUF design with 32 bit response paired among each other. Fig 25 shows the layout of a simple MUX PUF and Feed forward PUF array (16 test structures in a row) in 32nm SOI process. Fig. 26 shows the functional block diagram of the proposed circuit to measure the BER and frequency difference on-chip.

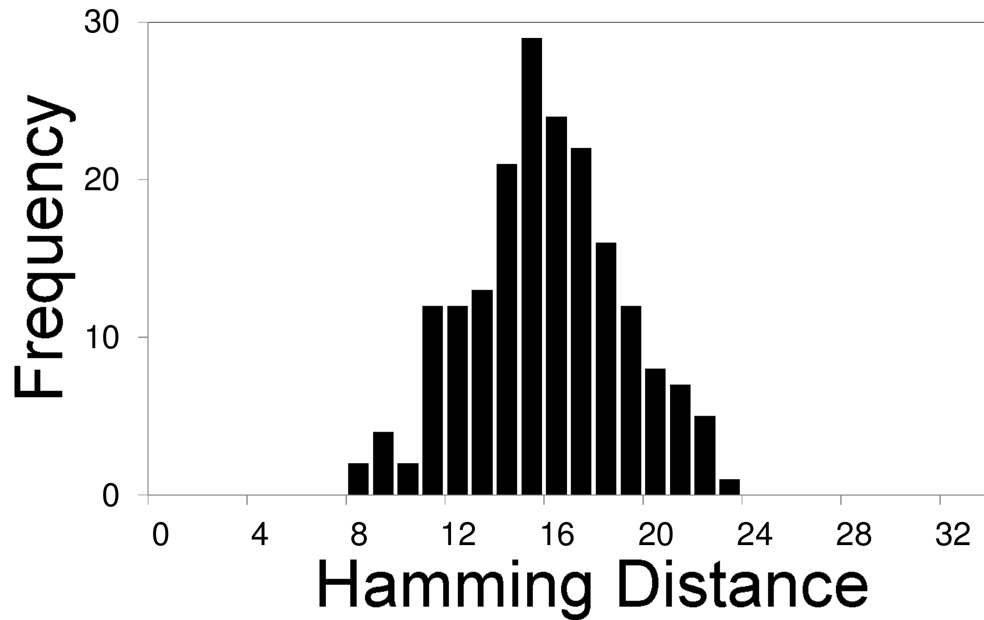


Figure 24 Hamming distance distribution of a post layout 32 stage feed forward reconfigurable PUF design with 32 bit challenge-response pair

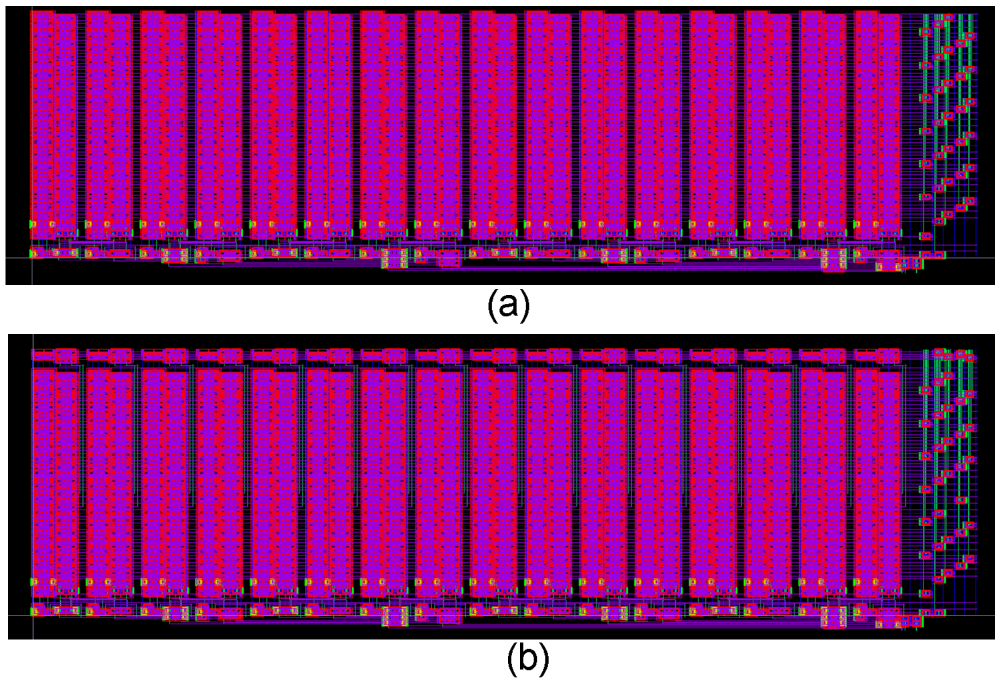


Figure 25 Layout of (a) General and (b) feed forward MUX PUF array in 32nm SOI process

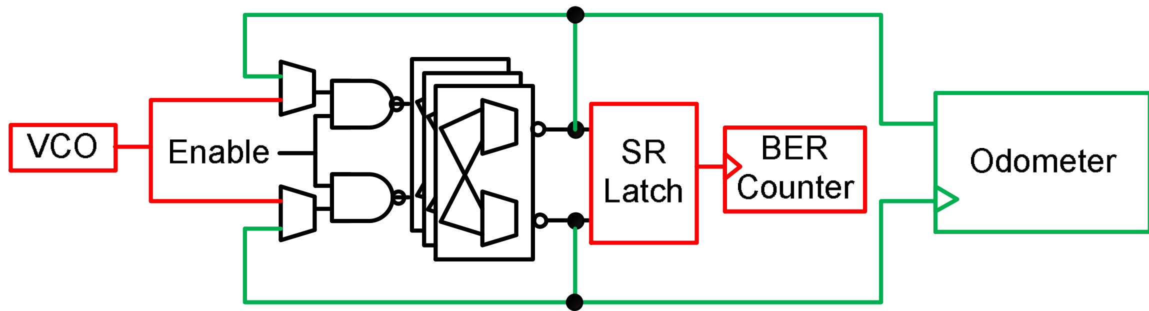


Figure 26 PUF with bit error rate (BER) and beat frequency difference (BFD) measurement blocks

XII. Summary

Due to the widespread use of DVFS technique in the modern processors, it is necessary to measure and characterize the guard-band during the supply ramp. Moreover, due to the adoption of state-of-art voltage regulators like iVRM in IBM processors [2] and FIVRs in Intel processors [3], the voltage ramp up time has reduced to sub-µs level. This has resulted in higher frequency fluctuations due to BTI aging and recovery. In turn, the worst-case guard-bands are becoming critical. So, it has become indispensable for the designers to study the BTI effect under fast DVFS transients. In this work, we built a revolving reference odometer based test chip that measures the frequency shift in fast DVFS environment. Due to the high measurement resolution, low measurement time, and fast measurement steps, for the first time the BTI degradation and recovery effects could be measured as early as 1µs after the power supply transition. Use of multiple fresh on-chip ROSCs also ensured reliable measurement data. The measurements were observed across different voltage, stress time duration, temperature and supply ramp duration. It was concluded that the BTI frequency shift due to supply transition increases with voltage difference transition, temperature and stress time duration, while it decreases with supply ramp time.

Bibliography

[1] Chen Zhou; Xiaofei Wang; Weichao Xu; Yuhao Zhu; Reddi, V.J.; Kim, C.H., "Estimation of instantaneous frequency fluctuation in a fast DVFS environment using an empirical BTI stress-relaxation model," Reliability Physics Symposium, 2014 IEEE International , vol., no., pp.2D.2.1,2D.2.6, 1-5 June 2014

[2] Toprak-Deniz, Z.; Sperling, M.; Bulzacchelli, J.; Still, G.; Kruse, R.; Seongwon Kim; Boerstler, D.; Gloekler, T.; Robertazzi, R.; Stawiasz, K.; Diemoz, T.; English, G.; HUI, D.; Muench, P.; Friedrich, J., "5.2 Distributed system of digitally controlled microregulators enabling per-core DVFS for the POWER8TM microprocessor," Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International , vol., no., pp.98,99, 9-13 Feb. 2014

[3] Kurd, N.; Chowdhury, M.; Burton, E.; Thomas, T.P.; Mozak, C.; Boswell, B.; Lal, M.; Deval, A; Douglas, J.; Elassal, M.; Nalamalpu, A; Wilson, T.M.; Merten, M.; Chennupaty, S.; Gomes, W.; Kumar, R., "5.9 Haswell: A family of IA 22nm processors," Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International , vol., no., pp.112,113, 9-13 Feb. 2014

[4] Teo, Z. Q.; Ang, D. S.; Du, G. A, "Observation of two gate stress voltage dependence of NBTI induced threshold voltage shift of ultra-thin oxynitride

gate p-MOSFET," Reliability Physics Symposium, 2009 IEEE International , vol., no., pp.1002,1004, 26-30 April 2009

[5] M. Basoglu, M. Orshansky, and M. Erez, “NBTI-Aware DVFS: A New Approach to Saving Energy and Increasing Processor Lifetime,” Proc. of IEEE International Symposium on Low-Power Design, pp. 253-258, Austin, TX, Aug. 2010.

[6] B. Zhang and M. Orshansky, “Modeling of NBTI-Induced PMOS Degradation under Arbitrary Dynamic Temperature Variation,” IEEE International Symposium on Quality Electronic Design (ISQED), pp. 774-779. San Jose, CA, March 2008

[7] Min Chen; Reddy, V.; Carulli, J.; Krishnan, Srikanth; Rentala, V.; Srinivasan, V.; Yu Cao, "A TDC-based test platform for dynamic circuit aging characterization," Reliability Physics Symposium (IRPS), 2011 IEEE International , vol., no., pp.2B.2.1,2B.2.5, 10-14 April 2011

[8] Keane, J.; Persaud, D.; Kim, C.H., "An all-in-one silicon Odometer for separately monitoring HCI, BTI, and TDDB," VLSI Circuits, 2009 Symposium on , vol., no., pp.108,109, 16-18 June 2009

[9] Keane, J.; Kim, C.H., "On-chip silicon odometers and their potential use in medical electronics," Reliability Physics Symposium (IRPS), 2012 IEEE International , vol., no., pp.4C.1.1,4C.1.8, 15-19 April 2012

[10] Bhargava, M.; Cakir, C.; Ken Mai, "Comparison of bi-stable and delay-based Physical Unclonable Functions from measurements in 65nm bulk CMOS,"

Custom Integrated Circuits Conference (CICC), 2012 IEEE , pp.1,4, 9-12 Sept. 2012

[11] Lim, D.; Lee, J.W.; Gassend, B.; Suh, G.E.; van Dijk, M.; Devadas, S, "Extracting secret keys from integrated circuits," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.13, no.10, pp.1200,1205, Oct. 2005

[12] Guajardo, J.; Kumar, S.S.; Schrijen, G.-J.; Tuyls, P., "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection," Field Programmable Logic and Applications, 2007. FPL 2007. International Conference on , vol., no., pp.189,195, 27-29 Aug. 2007

[13] Suh, G.E.; Devadas, S, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE , vol., no., pp.9,14, 4-8 June 2007

[14] Chi-En Yin; Gang Qu, "Improving PUF security with regression-based distiller," Design Automation Conference (DAC), 2013 50th ACM / EDAC / IEEE , vol., no., pp.1,6, May 29 2013-June 7 2013

[15] Ganta, D.; Vivekraja, V.; Priya, K.; Nazhandali, L., "A Highly Stable Leakage-Based Silicon Physical Unclonable Functions," VLSI Design (VLSI Design), 2011 24th International Conference on , vol., no., pp.135,140, 2-7 Jan. 2011

[16] Lao, Y.; Parhi, K.K., "Reconfigurable architectures for silicon Physical Unclonable Functions," Electro/Information Technology (EIT), 2011 IEEE International Conference on , vol., no., pp.1,7, 15-17 May 2011