Leveraging the Power Grid for Localizing Trojans and Defects

Jim Plusquellic
ECE, University of New Mexico, NM
jimp@ece.unm.edu

Dhruva Acharyya
Verigy Inc., Santa Clara, CA
dhruva.acharyya@verigy.com

Abstract

The finite, non-zero resistance of the metal wires that define the power grid of chips require the insertion of multiple ports between the grid and the external power supply in order to meet voltage stability requirements across the 2-D plane of the chip. The ports connect to the power grid along its edges for peripheral pad configurations, while, for C4 or array pad configurations, the ports are distributed across the 2-D surface of the chip. In either case, the availability of multiple power ports can be leveraged for detecting and localizing defects and/or Trojan circuits. A localization technique is investigated in this paper that analyzes anomalies introduced by defects and/or Trojans in the measured I_{DDQ}s from these ports. The localization accuracy of the technique can be improved significantly through the use of calibration and additional information collected from simulation experiments. The method and model are validated using data collected from a set of chips fabricated in an IBM 65 nm SOI process.[1]

Introduction

The functional and parametric behavior of integrated circuits (ICs) are increasingly impacted by manufacturing process variations and a wider variety of defect types as they are scaled into smaller nanometer regimes. The yield loss mechanisms are changing because of shrinking geometries, sub-wavelength lithography, and the use of new materials and processes. This is challenging the management of yield during ramp and during volume production. The dominant factors for yield loss in nanometer technologies are shifting from random defects to systematic design and process interactions effects. This requires a new approach to yield management techniques in modern technologies [1].

Quickly locating and diagnosing the root cause of failure is an becoming increasingly important component of yield management. Design phase techniques such as design for manufacturing (DFM), optical proximity correction (OPC), phase shift masks (PSM), short flow characterization vehicle (CV) and yield simulations are not sufficient and require support from yield monitors and yield loss analysis tools to identify root cause [2]. In order to diagnose design specific yield loss factors, it is necessary to gather yield loss information from structural test data.

Diagnosis is the process designed to identify the location of the fault in chips that have failed in the field or at production test [3]. It is carried out by processing failure information and then deducing a set of potential fault candidate sites on the chip. Volume diagnostics collects and analyzes structural test data in production over a significant volume to identify dominant yield loss areas on the chip. Efficient techniques for quickly and accurately localizing defects are an important component of volume diagnostic procedures.

Diagnosis is performed for three different purposes: 1) to improve the yield of first silicon; 2) to ensure high product quality during volume production; and 3) to analyze the reliability issues that cause customer returns [4]. The quality of a diagnostic algorithm is measured by its resolution, defined as the ratio of the number of true defects identified to the total number of reported candidates. More effective diagnostic tools achieve higher resolutions by reducing the number of candidate fault sites. Diagnosis is followed by failure analysis, which is a process carried out by a human analyst to verify the candidate sites. Poor resolution implies that many candidate must be investigated, increasing the cost of failure analysis. The process of diagnosing faulty chips is becoming more challenging because of higher transistor/wire densities and increasing chip areas susceptible to random particles.

A similar but distinct problem exists in the area of hardware security. A hardware Trojan is a deliberate and malicious modification to a chip's logic function that is designed to shutdown the chip at some pre-determined time and/or when some specific signal or data pattern is received [5][6]. The objective of the diagnostic technique in this case is to determine the physical, layout position(s) of the inserted Trojan gates.

[1]Chips designed while on sabbatical at IBM Austin Research Laboratory.

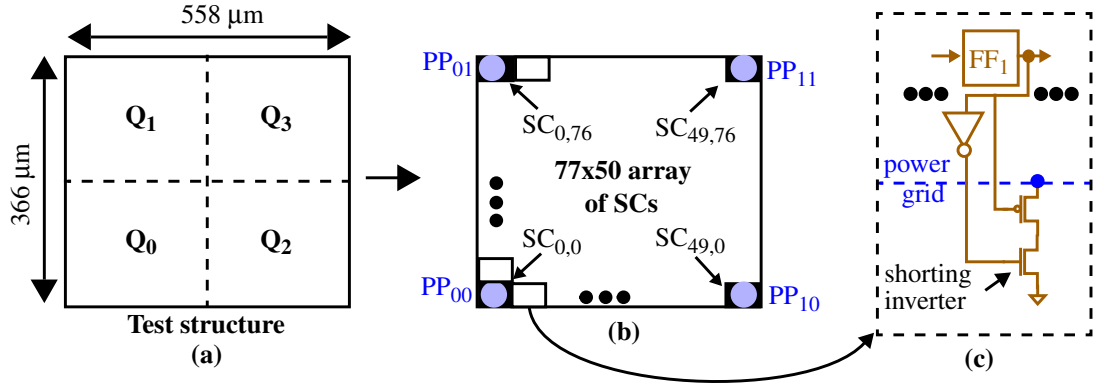

Figure 1: (a), (b) Block diagrams of the test structure and (c) details of stimulus circuit (SC).

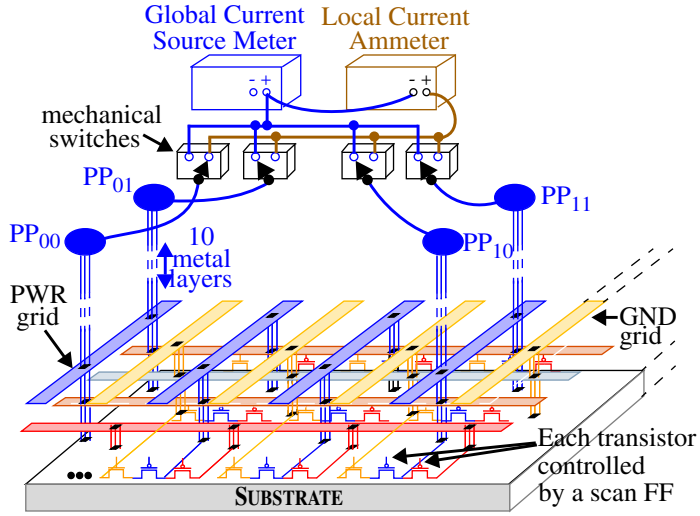

Figure 2: External Instrumentation Setup.

Several "software-based" diagnostic methods have been proposed based on I_{DDQ} measurements[1] [7-14]. These methods can be classified as static, quasi-static and dynamic diagnostic test paradigms. For static, the diagnostic test set and test response are precomputed and stored in a fault dictionary. The quasi-static paradigm, the test set is pre-computed but the fault dictionary is eliminated. Instead, the test response is computed dynamically. Under the dynamic paradigm, both the diagnostic test set and response are computed dynamically during response analysis.

The quiescent signal analysis (QSA) method that we propose in this work is an alternative approach to diagnosis and cannot be classified under these paradigms. It is complementary to these strategies and can be used in combination with them as a means of further improving diagnostic resolution. Moreover, QSA is more robust to the detrimental effects of increasing background leakage currents than other methods. This is true because, in QSA, the individual supply port currents are measured, in contrast to the global (chip-wide) I_{DDQ} measured by other methods. The partitioning of the global leakage current across the multiple supply ports of the chip reduces its magnitude in each of the supply port measurements.

In [15], we proposed a hyperbola-based diagnostic method that is able to "triangulate" a defect's location to a physical position in the layout of the chip. The method accomplishes this by computing the parameters for a pair of hyperbolas from the I_{DDQ}s measured at neighboring supply ports. The intersection of the hyperbolas identifies the predicted location of the defect in the layout. In this paper, a new exponential model is developed that provides a higher level of localization accuracy and is applicable over a wider range of PG architectures. We apply this technique to a set of chips fabricated in a 65 nm SOI technology and show that 95% of the emulated defects can be located to a region less than 12 microns in diameter.

Test Chip Design and Experiments

This section covers the design of the chips used in the defect/Trojan emulation experiments[2].

Test Chip Design

A block diagram of the test structure design is shown in Fig. 1(a) and (b). It consists of a 77x50 array of stimulus circuits (SCs) that occupies an area 558 µm wide and 366 µm high. Each SC consists of a flip-flop connected in a scan chain and a *shorting inverter*, as shown in 1(c). Given this configuration, a short between the power and ground grid in metal 1 can be introduced by enabling any one of 3,850 (77x50) shorting inverters in a selected SC using the scan chain. The power (PWR) grid is connected to an external power supply through 4 power ports (PPs) (C4 bumps that tie into metal 10 on the PWR grid), labeled in Fig. 1(b) as PP_{00} through PP_{11}.

Fig. 2 shows the external instrumentation setup. The PPs wire out of the chip on separate pins in the package. The individual power pins are each wired to a low resistance mechanical

[1] I_{DDQ} refers to the quiescent power supply leakage current of an IC.

[2] We replace the term 'defect/Trojan' with 'defect' in the remainder of the paper for clarity. without loss of generality.

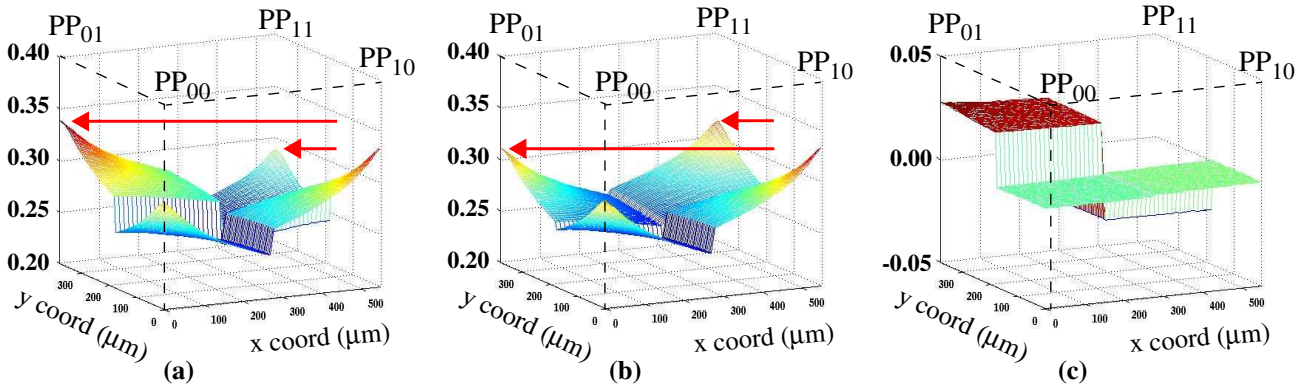

Figure 3: Normalized branch currents for Chip #1 (a) and Chip #2 (b) and their differences (c).

switch as shown along the top portion in Fig. 2. The switch can be configured in a left or right position. The left and right outputs of the switches connect to a common wire that routes to the *global current source meter* (GCSM) and *local current ammeter* (LCA), respectively.

The GCSM provides 0.9 V to the PWR grid and can measure current with a resolution less than 300 nA. The LCA is wired in series with the GCSM and allows measurement of the individual power port (local) currents at the same level of resolution. For example, the switch configuration in Fig. 2 allows measurement of the local PP_{00} current, I_{00}, as well as the global current.

Current Profiles

On the surface, it appears that using a set of PP currents could be very effective for localizing defects because the distributed nature of the PPs enable a two dimensional analysis to be carried out. However, several challenges must be dealt with in order to leverage the full potential of the method. The first major challenge is dealing with process and environmental variations effects. Process variations, such as associated with non-ideal CMP, introduce resistance variations in the metal layers defining the PWR grid. Resistance variations change the current distribution characteristics to the power ports on a chip-by-chip basis. The low impedance nature of the PWR grid makes current distribution extremely sensitive to even small, i.e., less than 1 Ohm, resistance variations. Similarly, series resistance variations, i.e., those associated with the conductors between the external power supply and the power ports, and the probe card, also have dramatic effects on current distribution characteristics.

This is illustrated using the plots in Fig. 3, which displays the PP currents collected from two chips. The data was collected using the following process. The currents, I_{00} through I_{11}, from each of the four PPs were measured as each of the 3,850 shorting inverters were enabled, one at a time, across the 2-D array of SCs (see Fig. 1b)[1]. The four currents from each SC were then divided by the *sum* of the four currents (the **global** current). This process, called **normalization**, effectively removes the variations in the currents introduced by process variation effects within the shorting inverters themselves. The normalized currents, each expressed as a fraction between 0.0 and 1.0, reflect only PWR grid resistance variations and noise.

The plots in Fig. 3 are constructed by 'pasting' the normalized PP currents measured from the subset of SCs in each region or *quad* surrounding the PP, labeled as Q_x in Fig. 1(a). Each quad includes 3850/4 = 962 SCs. For example, the left side of Fig. 3(a) plots the normalized PP_{01} currents from SCs in Q_1. By pasting together the current profiles from each of the PPs, it becomes easy to see the systematic variations that exists between the PPs of the individual IC. For example, the maximum normalized current for PP_{01} is approximately 0.33 as indicated by the arrow in Fig. 3(a) while the maximum for PP_{11} is closer to 0.3. For reasons described in the following sections, localization accuracy is maximized when the maximum values across all PPs are the same. One of our objectives will be to develop a method that calibrates the measured currents to achieve this goal.

Another important artifact that is evident in these plots is that the systematic resistance variations are different for each of the chips. For example, the relative ordering of the maximum values for PP_{01} and PP_{11} are reversed for the second chip's data shown in Fig. 3(b) when compared with 3(a). Fig. 3(c) plots the differences that exist between the plots in Fig. 3(a) and (b). A key objective of our calibration technique will be to 'normalize' these systematic resistance variations between chips, effectively making the current profiles for all chips as similar as possible. Once calibrated, an analytical model for localization can be developed that is applicable to ANY chip in the population.

The calibration procedure requires the insertion of calibration circuits (CCs), identical to those shown in Fig. 1(c), in the chip at specific layout positions [16]. The layout positions that yield the best results are shown by the darkly shaded rectangles directly under the circular PPs in Fig. 1(b). The SCs at these

[1]The leakage current measured through each of the PPs is removed from the shorting current measurements by subtraction.

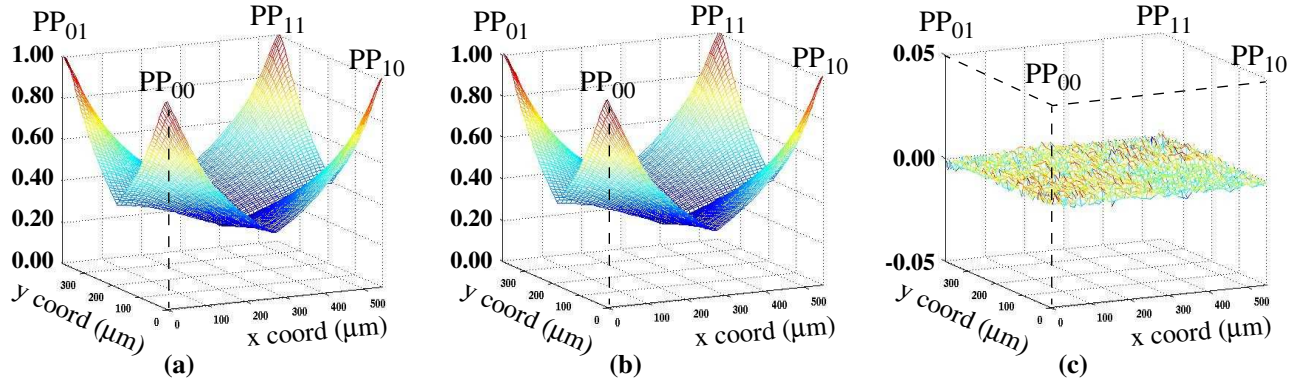

Figure 4: Calibrated normalized branch currents for Chip #1 (a) and Chip #2 (b) and their differences (c).

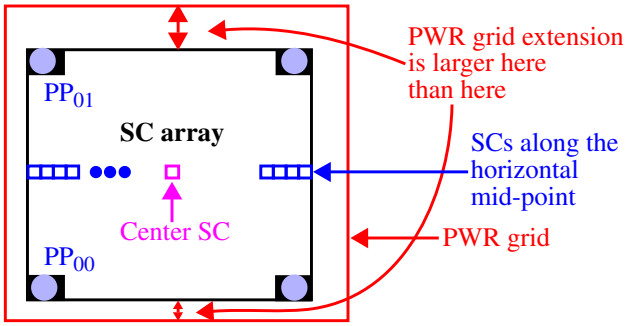

Figure 5: Actual power (PWR) grid architecture in the test chips.

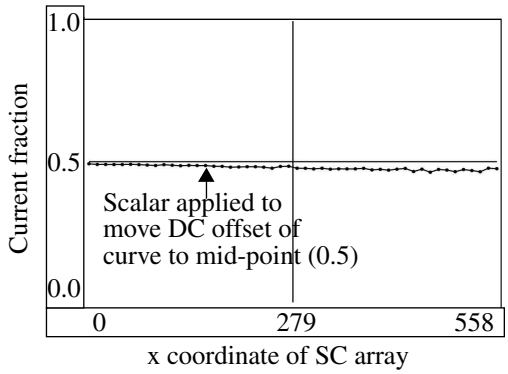

Figure 6: Distortion in the current distribution to PPs introduced by PWR grid architecture.

positions serve as CCs in our calibration procedure. A set of calibration tests are performed on a chip by enabling, one at a time, each of the CCs and measuring the branch current, I_{xy}, through each of the PP_{xy}s. The data collected from the four CC tests defines a calibration matrix, which is used in a linear transformation operation to significantly reduce process and environmental chip-to-chip variations. Details of the calibration procedure can be found in [15][16].

The effect of calibration is dramatic as shown by the plots in Fig. 4, which shows the calibrated versions of the normalized current profiles given in Fig. 3. The first obvious change is the maximum values at each of the PPs are all equal across the PPs of both chips. More importantly, the differences between the profiles, as shown in Fig. 4(c), are nearly zero. All that remains in the difference profile are variations introduced by measurement noise. Clearly, calibration achieves our first major objective, i.e., to make the current distribution profiles of every chip as similar as possible.

Fixing Power Grid Architecture-related I_{DDQ} Anomalies

The architecture of the PWR grid also has a large impact on the achievable resolution of our localization method. An ideal PWR grid is one that is perfectly 'symmetrical' around its power ports. The power port I_{DDQ}s in a symmetrical grid are consistent and predictable, and facilitate the development of analytical models designed to predict their behavioral characteristics. On the other hand, non-symmetries in the PWR grid architecture distort I_{DDQ} distributional characteristics to the PPs, requiring a second form of 'calibration' in order to achieve good results using a predictive analytical model. We describe one technique (of many possible solutions) to deal with this challenge below.

The block diagram in Fig. 5 shows the non-symmetries in the PWR grid architecture of our test chips. The SC array is shown as a rectangle within a larger rectangle that represents the extent of the PWR grid. The extension of the PWR grid beyond the edge of the array is larger along the top portion of the array than it is along the bottom portion. A similar 'offset' occurs on the left and right edges of the array. The asymmetry in the alignment of the PWR grid with power ports and core logic distorts the distribution of current to the power ports in a non-linear fashion. The calibration process described in the previous section cannot 'fix' this type of distortion and therefore, another strategy is needed. Bear in mind, there are many other types of PWR grid architecture distortions. For example, even in a scenario in which the PWR grid is precisely aligned with the edges of the core logic, larger grids with more than 4 power ports have 'edge effects', i.e., current distortions in portions of the PWR grid along the edges of the core logic.

An easy way to demonstrate the impact of this non-linear distortion is to plot the I_{DDQ}s from the SCs along a straight line in the SC array. In Fig. 6, we plot *current fractions*, using I_{00} (from PP_{00}) and I_{01} (from PP_{01}) for the SCs along the horizontal mid-point shown in Fig. 5. Current fractions are defined by Eq. 1, where I_{00} is *normalized* on the right by dividing by the

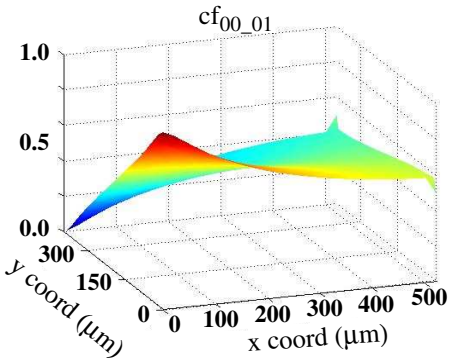

Figure 7: Current fractions, cf_{00_01}, for 10 layer PWR grid model of chips.

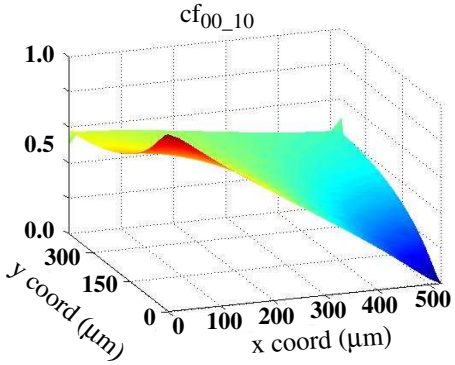

Figure 8: Current fractions, cf_{00_10}, for 10 layer PWR grid model of chips.

sum of two I_{DDQ}s, $I_{00} + I_{01}$, measured at PP_{00} and PP_{01}. The

$$cf_{00\_01} = \frac{I_{00}}{(I_{00} + I_{01})} \quad (1)$$

notation cf_{a_b} represents the current fraction for two power ports with coordinates given by *a* and *b*.

In a symmetrical grid, the expected current fraction is 0.5. Although the curve from our experiments is close to 0.5, it is offset slightly downward (and is actually non-linear). The DC component of this offset, as well as the offset that occurs between horizontal pairings of PPs (not shown), can be easily fixed by computing a set of scalars from simulations of the PWR grid. In particular, an SC in the center of the grid can be simulated (see Fig. 5) and a simple set of linear equations can be solved to obtain the factors. The PP currents measured from the chips can be multiplied by these factors, effectively moving the entire curve upward as shown in Fig. 6. Fixing both the DC and non-linear components requires a more complex process, which is currently under investigation and will be described in a future work.

Current Fractions

Our ultimate goal is to develop an analytical model that describes the current distribution of PGs accurately, so that such a model can be used to predict the location of shorting defects. One approach is to develop a model using the distribution of the currents as shown in previous figures, i.e., using the supply port currents directly. A second approach is to develop a model based on normalized current fractions, as defined earlier using Eq. 1.

We refer to the normalization given by Eq. 1 as *local normalization*. Local normalization has several advantages over an approach that uses the un-normalized currents directly or an approach that uses *global normalization*, where the denominator is the sum of all power port currents. First, any form of normalization, by definition, replaces the actual magnitude of the current with a relative quantity. This is an advantage for techniques such as defect localization, which ideally should predict the same location for a defect independent of how much current the defect draws from the PG. Second, the local form of normalization defined by Eq. 1 is less sensitive to noise than global normalization, because the source of noise in the former originates from only two power port measurements while the source of noise in the latter is chip-wide. Last, local normalization decomposes the current distribution characteristics imposed by the PG into orthogonal, x and y components. For example, the current fraction, cf_{00_01} as defined by Eq. 1 represents the y dimension because it is computed using vertically oriented power ports, PP_{00} and PP_{01}, as shown in Fig. 1. The x dimension could be represented using a second current fraction defined as cf_{00_10} in Eq. 2. This type of decomposition enables

$$cf_{00\_10} = \frac{I_{00}}{(I_{00} + I_{10})} \quad (2)$$

methods designed to 'triangulate' to the position of the defect, as described in the following paragraphs.

The key to accurately predicting the position of a defect from PP current measurements is determining the relationship between the position of a defect in the layout, i.e., the point at which the defect draws current from the PG, and the corresponding values of the current fractions, e.g., such as those defined by Eq. 1 and 2. Fig. 7 plots the magnitude of the current fraction cf_{00_01} along the z axis for a set simulation experiments, each configured with a current source attached to the PG at the position given by the x and y dimensions of the plot. The current source in each experiment is configured to sink 1 mA at the attachment point, which is made in metal 1 layer on a 10 layer PG model derived from the chip's test structure. Fig. 8 plots the relationship for cf_{00_10}. The simulation data is calibrated as described above. Calibration expands the range of measured values by eliminating the *wash-out* effect introduced by the vertical resistance in the PG and any resistance in series with the PPs and the power supply. This range expansion causes a corresponding expansion in the range of the current fractions from 0.0 to 1.0, as seen in the plots.

A second *contour curve* view of the current fraction data is shown in Fig. 9 and 10. The *contour curve* view flattens the z dimension of the 3-D plots by color coding the magnitude component into the 2-D plane. The region between a pair of contour curves identifies the (x,y) locations in the layout where

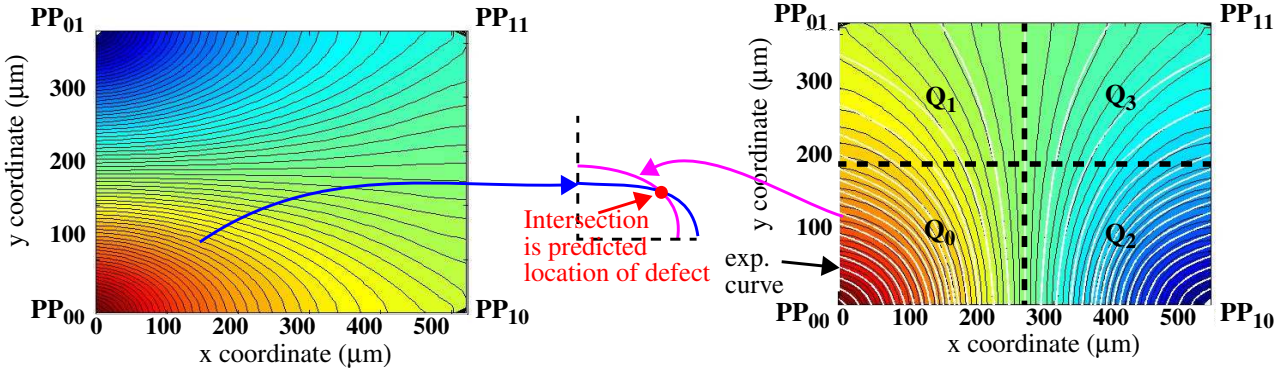

Figure 9: Current fractions contour curves, cf_{00_01}, from Fig. 7.

Figure 10: Current fractions contour curves, cf_{00_10}, from Fig. 7 plus superimposed exponential curves.

current sources, i.e., shorting defects, produce nearly equal values of the current fraction. The regular, elliptical shape of the curves suggest that it may be possible to derive a simple function that approximates their behavior. The functions derived for the contour curves from two orthogonally adjacent pairing of PPs, e.g., those shown in Fig. 9 and 10, can be used to predict the location of a defect. This is accomplished by computing the curve associated with each function, using the measured current fractions as parameters, and then computing their intersection. The center portion of Fig. 9 and 10 shows an example where one of the contour curves is 'selected' from each plot. The intersection of the two curves serves as an estimate of the defect's location.

In previous work, we used a hyperbola equation to approximate these curves [15]. In this work, we investigate the use of an exponential function and show a significant improvement in the accuracy of the predicted location of defects in comparison to the hyperbola model. However, the exponential model requires several additional parameters to be specified, beyond the measured current fractions themselves. Simulation experiments are required to determine the value of these parameters, as described below.

Fig. 10 shows a set of exponential curves superimposed on the contour curves. Although they are not an exact match, the exponential curves track the contours fairly well particularly in the lower left region of the figure labeled Q_0 (The limits of Q_0 are given by the dotted lines in the plot.) Accurately tracking the contour curves outside of Q_0 is not important because we use the contour curves from a different pair of orthogonally adjacent PPs for the other regions.

Exponential Model

An exponential curve has three parameters that need to be determined from the measured currents. These parameters are labeled as ***x-offset***, ***y-offset*** and ***curvature*** on the exponential curve shown in Fig. 11. The x-offset and y-offset represent the displacement of the exponential from the origin while the *curvature* parameter represents its scaling in the y dimension. The

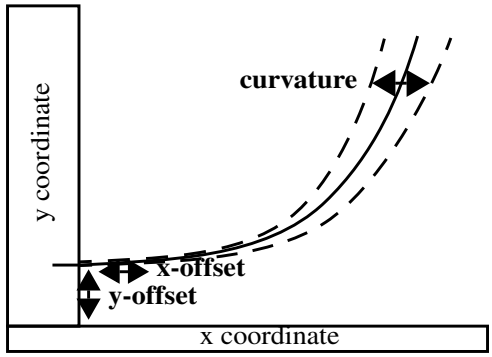

Figure 11: Exponential Curve and Parameters.

equation of an exponential that incorporates these parameters is given in Eq. 3.

$$y = e^{(x * \text{curvature} + \text{x\_offset})} + \text{y\_offset} \qquad (3)$$

The y-offset parameter gives the vertical offset of the curve from the origin as shown in Fig. 11. The exponentials shown in Q_0 of Fig. 10 are rotated 90 degrees counter-clockwise and therefore the y-offset parameter denotes a distance along the x-axis from the origin given in the lower left corner at (0, 0). In either case, the y-offset parameter corresponds to the intersection of the exponential with a line drawn between the appropriate pairing of PPs. For Fig. 10, the PPs are PP_{00} and PP_{10}.

In order to derive the y-offset, we must first determine the relationship between current fractions and the (x,y) location of a current source in the layout. Fig. 12 plots this relationship from simulations using a PG model of the chips superimposed on the curves obtained from the actual chips. The simulation-derived current fractions cf_{00_10} are computed using data generated from a sequence of simulation experiments. In each simulation, a current source is inserted at an (x,y) location along the line between PP_{00} and PP_{10}. The currents measured at PP_{00} and PP_{10} are used to compute the corresponding cf_{00_10} using Eq. 2, which is plotted against the x coordinate of the enabled current source in the figure. A similar process was carried out for the chips to generate the superimposed curve data.

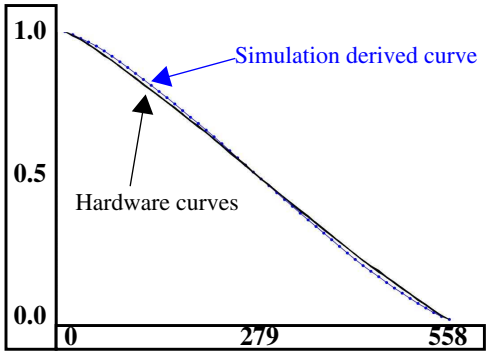

Figure 12: Hardware and simulation derived y-offset parameter for PP_{00}-PP_{10} pairing.

In this case, a subset of the SCs, i.e., those along the line between the power ports, were enabled one at a time. These curves serve as a mapping function between the measured current fractions and an (x,y) position of a current source along the line between the PPs.

The curvature parameter of exponential curves is derived using a second subset of SCs (for chips) and inserted current sources (for simulations), at positions shown by the dotted lines in Fig. 13 for the PP_{00}-PP_{10} pairing. The simulation and hardware data curves are shown in Fig. 14. The y-offset parameter for each experiment is plotted along the x axis and the corresponding curvature parameter is plotted on the y-axis. The curvature parameter is obtained by solving Eq. 3 for the curvature parameter using the y-offset and the (x,y) position of the inserted current source. These curves also serve as a mapping function between a y-offset parameter (obtained from Fig. 12) and a corresponding curvature parameter. Therefore, each measured current fraction has a unique y-offset and curvature parameter that define an exponential curve.

The value of the x-offset parameter of Eq. 3 was determined by curve fitting the exponentials to the contour curves, such as those shown in Fig. 10. The computed value of 2.5 remained constant for all exponential curves. The accuracy of the localization process is relatively insensitive to this parameter, and therefore, precisely determining it is not important in practice.

The y-offset curves of the chips shown in Fig. 12 are indistinguishable, which reflects the effectiveness of the calibration technique in making all chip data nearly identical. In contrast, the simulation derived y-offset curve, although a good match to the hardware, has a more noticeable reverse 's-shape' associated with it. This small difference is responsible for most of the localization error reported in the last section of this paper.

The curvature parameter curve shown for the hardware data in Fig. 14 is the average of the curves derived from the chips. The asymmetry in the curve around the center x coordinate 279 is caused by the asymmetry in the architecture of the PWR grid, as described above in relation to Fig. 5.

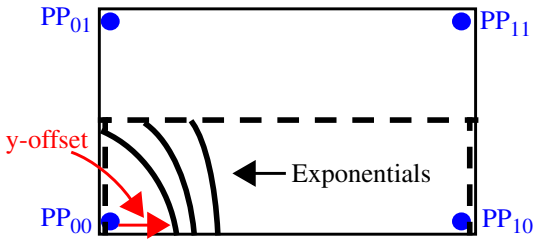

Figure 13: Dotted lines give positions in the PG model of the chip used to derive curvature parameter data.

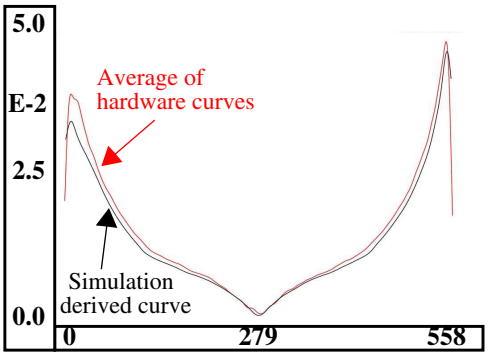

Figure 14: Hardware and simulation derived curvature parameter for PP_{00}-PP_{10} pairing.

Diagnosis

Hardware and Simulation Data Analyses

A key objective of our localization method is to use simulation experiments on a model of the chip's PWR grid to derive the y-offset, curvature and x-offset parameters to the exponential curves described above. Localization accuracy is therefore tied to the accuracy of the PG model. In our experiments, only limited information was available concerning the resistance values of the metal and via layers for 65 nm process. This resulted in small differences between the simulation-derived and chip-derived curves, as shown in Fig. 12 and 14, and introduced error in the localization results. We determine the impact of this error by performing the analysis twice, once using simulation data to derive the curves and once using actual chip data. Note that the latter scenario is not possible in practice, and is used here solely to determine the best possible result.

In addition to these two trials, we also carried out an analysis called 'scaled', in which we compute a set of scaling constants that are used as multipliers for the simulation derived curves. From Fig. 12 and 14, it is clear that the simulation and hardware curves are very similar in shape and that most of the differences between them can be eliminated by multiplying them by a constant. Bear in mind that in an actual application, it may be possible to use process and in-line data to construct accurate simulation models, thereby avoiding the need to correct the curves in this fashion.

The appropriate scaling constants can be computed from the hardware and simulation curves directly in our experiments. In an actual application, however, the hardware curves would not

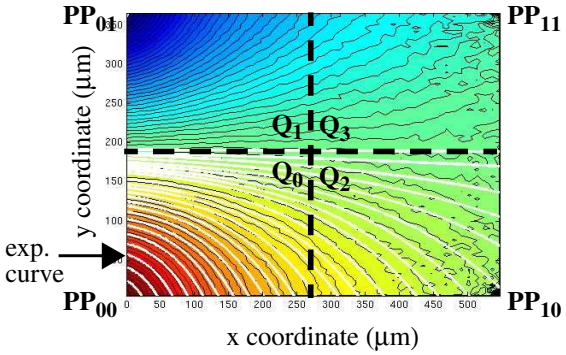

Figure 15: Chip C1 current fraction contours for PP_{00}-PP_{01}.

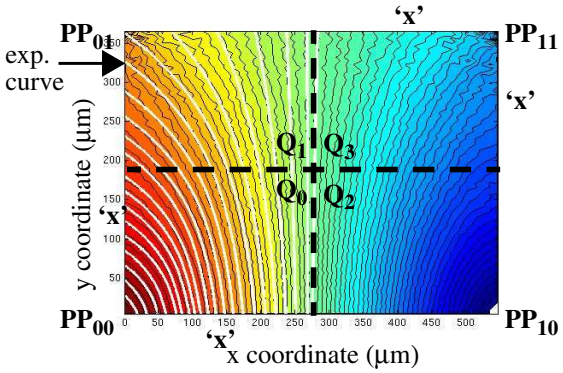

Figure 16: Chip C1 current fraction contours for PP_{00}-PP_{10}.

be available, and therefore, another approach is required. The constants cannot be determined from the currents measured from the calibration circuits described earlier (which are designed to eliminate process variation effects). This is true because after calibration, the currents from the calibration tests on the chips and simulation model are identical (which is the whole point to calibration).

Therefore, additional copies of the calibration circuits are needed to obtain these constants, with the additional copies best placed at positions shown by the 'x's in Fig. 16. These positions in the layout correspond to positions on the x-axis in Fig. 12 and 14 that are approximately 1/4th the distance along the x-axis, i.e., at 140 µm for PP pairing PP_{00} and PP_{10} in Fig. 16. These points on the x-axis correspond to places where the differences in the simulation and hardware curves are largest. The scaling constants are defined as the ratio of the currents measured in the simulation to those measured in the hardware experiments[1]. In our experiments, we used the SCs at these positions to compute a set of scaling constants and applied them to the simulation derived curves. The localization results using the scaled versions of the y-offset and curvature curves are given in the analysis labeled 'scaled simulation' described below.

Fig. 15 and 16 show the cfs_{00_01} and cfs_{00_10} contours for Chip C1, respectively. Two families of exponential curves are superimposed on the bottom-most and left-most contour curves, respectively. The parameters for these curves were derived from the hardware data directly. It is clear they are a good match to the underlying contour curves. This is reflected in the next section in the small level of localization error that occurs when the hardware-derived exponential curve parameters are used.

[1]When scaling the y-offset simulation curve in Fig. 12, the curve is first subtracted from a straight line that passes through the two end points of the curve. After scaling, the y components of the straight line are added back to the y-offset curve.

Results

A set of defect emulation experiments was performed on each chip by enabling, one at a time, each of the shorting inverters. For each experiment, the global and local I_{DDQ}s from the four supply ports were measured. This process produced 3,850 data sets for each chip (77 rows * 50 columns), where each data set consists of four PP I_{DDQ}s and one global I_{DDQ}. In total, we collected 69,300 emulated defect data sets from a set of 18 chips.

We evaluate our localization algorithm on these data sets. The algorithm estimates the (x,y) layout position of an enabled shorting inverter by generating two exponential curves, one from each pairing of orthogonal supply pads. For example, for shorting inverters in quad Q_0 of Fig. 15 and 16, an exponential curve is derived using the supply port pairing PP_{00}-PP_{01} and PP_{00}-PP_{10}. The parameters of the exponentials are obtained from the y-offset and curvature parameter curves derived under three different analyses; 1) a simulation analysis, 2) a 'scaled' simulation analysis and 3) a chip analysis. Once the exponential curves are generated, an estimate of the position of the shorting inverter is determined by computing the intersection of the two curves (similar to the process shown in the center of Fig. 9 and 10).

As an example, Fig. 17 shows 3-D plots of the localization error produced under these three analyses for chip C1. Localization error is computed as the Euclidean distance between the position of the enabled shorting inverter and the point of intersection of the exponential curves, and is reported in microns (µm). The results using simulation derived y-offset and curvature curves are given in Fig. 17(a). It is clear that the error surface is diverse with large errors (up to 60 µm) for SCs along two of the edges of the array and small errors (approx. 1 µm) for SCs in the center. In contrast, the errors produced in the chip analysis in Fig. 17(b) are uniform and much smaller, i.e., most are less than 10 µm. The similarity of these results to those shown in Fig. 17(c) under the 'scaled' simulation analysis illustrate that most of the error is due to a mismatch of the simulation model to the hardware. More importantly, the small

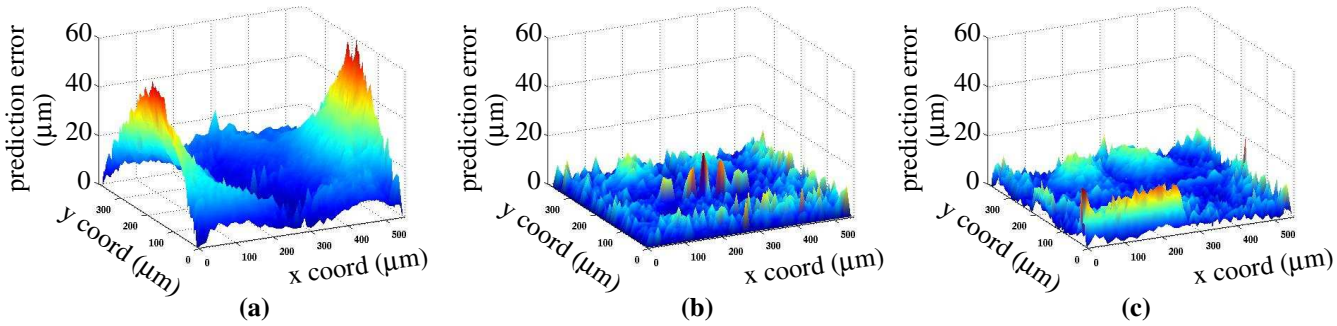

Figure 17: Localization errors for Chip C1 using a) simulation data, b) hardware data and c) 'scaled' simulation data.

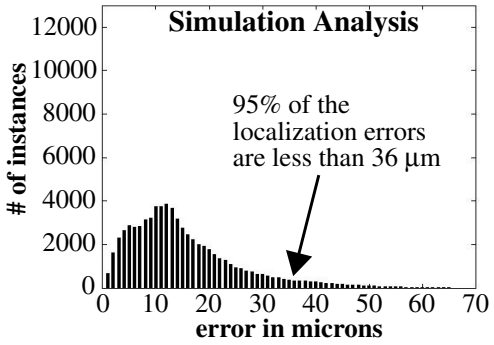

Figure 18: Localization errors using y-offset and curvature parameters derived from simulations.

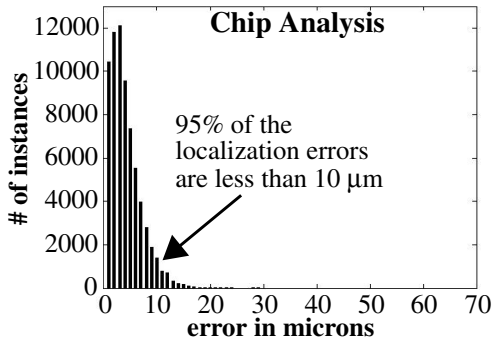

Figure 19: Localization errors using y-offset and curvature parameters derived from each chip.

errors in the latter two results confirm that the current contours are well modeled using exponential curves.

The histogram shown in Fig. 18 portrays the localization error across all 18 chips. The x axis bins the localization error in µm. The y axis gives the number of elements in each bin. For example, bin 1 contains 665 elements (which represent individual SC experiments), all of which have localization errors in the range of 0 to 1 µm.

The distribution of error in this histogram resembles a skewed gaussian with a long tail. The larger errors occur for SCs along the edges of the SC array, as discussed earlier in reference to Fig. 17(a). As indicated in the figure, 95% of the localization errors are bounded within 36 µm. Approximately 37% are within 10 µm.

The histograms shown in Fig. 19 and 20 report the errors in the analysis when the exponential parameters are derived from the y-offset and curvature parameter curves from each chip and from scaling the simulation curves, respectively. The results of the analysis shown in Fig. 19 are not obtainable in a practical application of our method, and we present them only to illustrate the best localization accuracy that can be achieved using this model. The distribution of error in this case is skewed far to the left (to smaller localization errors) and has a smaller tail. The 95% limit is reduced to 10 µm, and the 99% limit is at 13 µm. The bounds for the 'scaled' simulation results in Fig. 20 are given as 12 µm for the 95% limit and 17 µm for the 99% limit. This shows that it is possible to obtain much better

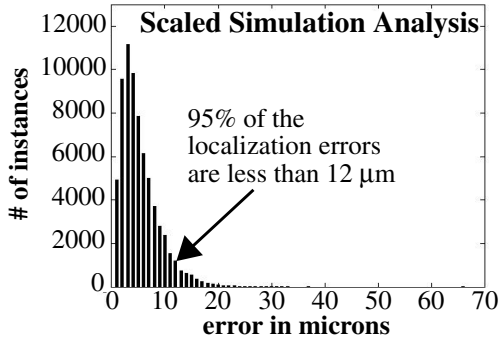

Figure 20: Localization errors using y-offset and curvature parameters from scaling the simulation curves.

results if an accurate simulation model is available or if additional 'calibration' circuits are inserted.

Summary and Conclusion

An exponential-curve model for defect and Trojan localization is proposed in this paper. The results demonstrate that it is possible to use I_{DDQ} to obtain an accurate estimate of the physical (x,y) layout position of where a defect sources current from the PWR grid. We also showed that calibration can remove many important resistance variations in the PDS. The localization error associated with the new model is reduced from the worst case of 140 µm using a hyperbola model to less than 60 µm [15]. The careful construction of a simulation model can reduce this worst case significantly, approaching a best case, worst case limit of approximately 25 µm.

Acknowledgments

We would like to thank Sani Nassif of IBM Austin Research Laboratory for the opportunity to build and conduct experiments on chips fabricated at IBM.

References

[1] ITRS (http://public.itrs.net/)

[2] J. Kibarian, "The Nature of Yield Ramping: Keeping Ahead of the Evolution", *International Test Conference*, 2005 keynote address.

[3] S. Venkataraman and S. B. Drummonds, "POIROT: A Logic Fault Diagnosis Tool and its Applications," *International Test Conference*, 2000, pp. 253-262.

[4] V. J. Mehta, M. Marek-Sadowska, Tsai Kun-Han and J. Rajski, "Timing-Aware Multiple-Delay-Fault Diagnosis", *Trans. on Computer-Aided Design of Integrated Circuits and Systems*, Vol.: 28, Issue: 2 , 2009, pp. 245-258.

[5] http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf

[6] J. Aarestad, D. Acharyya, R. Rad, and J. Plusquellic, "Detecting Trojans Though Leakage Current Analysis Using Multiple Supply Pad IDDQs", *Trans. on Information Forensics and Security*, 2010.

[7] Gong Yiming, S. Chakravarty, "Using Fault Sampling to Compute I_{DDQ} Diagnostic Test Sets", *VLSI Test Symposium*, 1997, pp. 74-79.

[8] S. Chakravarty, M. Liu, "I_{DDQ} Measurement Based Diagnosis of Bridging Faults", *Journal of Electronic Testing: Theory and Applications*, Vol. 3, 1992, pp. 377-385.

[9] I. Pomeranz and S. M. Reddy. "On the Generation of Small Dictionaries for Fault Location", *International Conference on Computer-Aided Design*, 1992, pp. 272-279.

[10] Aitken, R.C., "A Comparison of Defect Models for Fault Location with Iddq Measurements", *International Test Conference*, 1993, pp. 1051-1060.

[11] Y. Gong and on S. Chakravarty, "On adaptive Diagnostic Test Generation, *International Conference on Computer-Aided Design*, 1995, pp. 181-184.

[12] P. Nigh, D. Forlenza, F. Motika, "Application and Analysis of IDDQ Diagnostic Software", *International Test Conference*, 1997, pp. 319-327.

[13] C. L. Henderson and J. M.Soden, "Signature Analysis for IC Diagnosis and Failure Analysis", *International Test Conference*, 1997, pp. 310-318.

[14] C. Thibeault, L. Boisvert, "Diagnosis method based on delta IDDQ probabilistic signatures: Experimental results", *International Test Conference*, 1998, pp. 1019-1026.

[15] J. Plusquellic, D. Acharyya, M. Tehranipoor and C. Patel, "Triangulating to a Defect's Physical Coordinates Using Multiple Supply Pad IDDQs: Test Chip Results", *International Symposium on Testing and Failure Analysis*, Nov. 2006, pp. 36-45.

[16] D. Acharyya, J. Plusquellic, "Calibrating Power Supply Signal Measurements for Process and Probe Card Variations", *IEEE International Workshop on Current and Defect Based Testing*, 2004, pp. 23 - 30.

[17] R. M. Rad, W. Xiaoxiao, M. Tehranipoor, J. Plusquellic, "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans", *International Conference on Computer-Aided Design*, Nov. 2008, pp. 632-639.