SAND2016-3876C

Electronic Forensic Techniques for Manufacturer Attribution

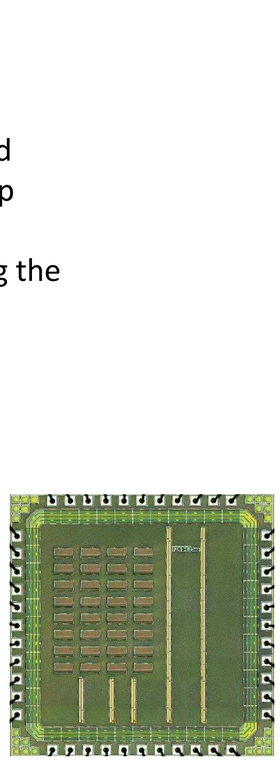
Ryan Helinski*, Edward Cole Jr.*, Gideon Robertson*, Jonathan Woodbridge, Lyndon Pierson
*Sandia National Laboratories
Albuquerque, New Mexico 87123
E-mail: rhelins, coleei, garobe@sandia.gov

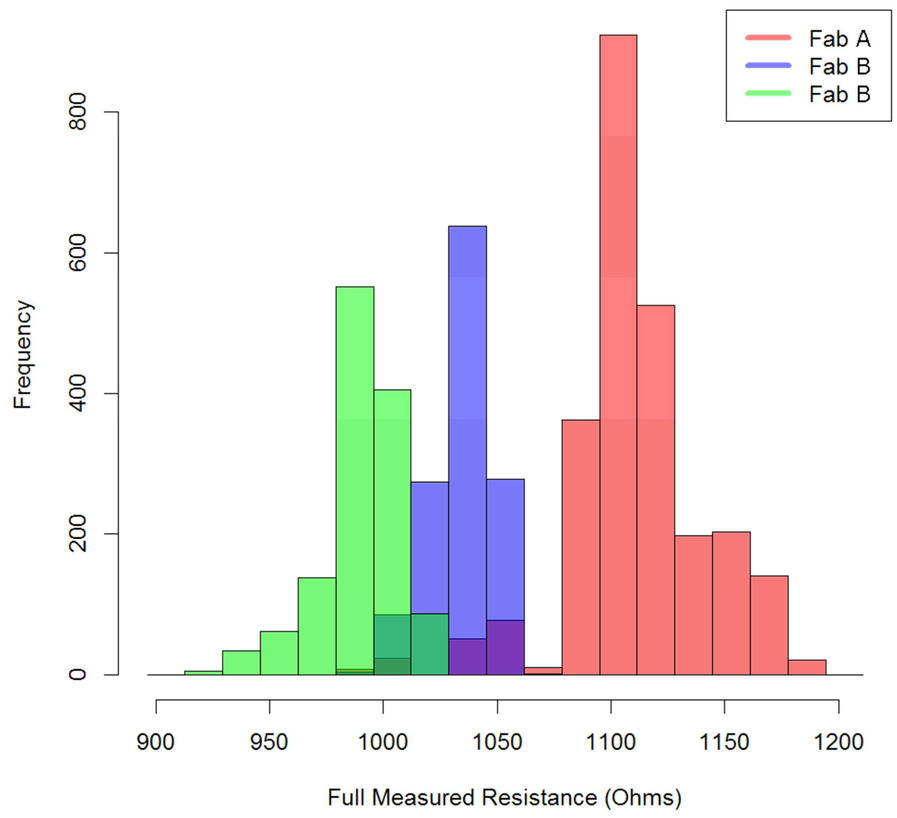
Introduction

The microelectronics industry seeks tools that can verify the origin of and track integrated circuits (ICs) through their lifecycle. Such tools could help detect counterfeit ICs and other issues. The focus of this work is on characterizing microelectronics fabs using on-chip circuits and estimating the fab prediction accuracy.

In the paper, we present novel techniques
- to measure multiple distinct manufacturing process variations
- using self-contained, on-chip circuits

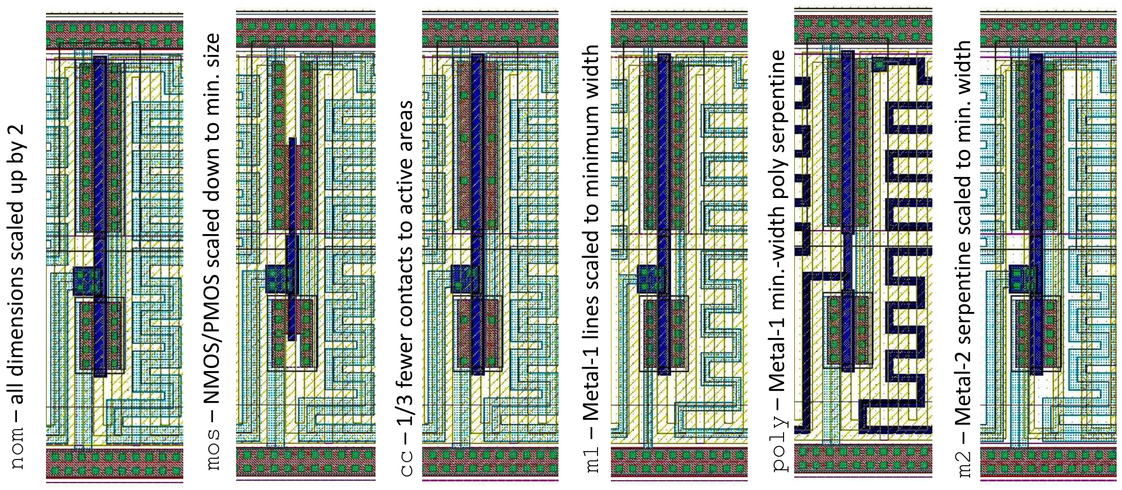
We present our analysis of 159 silicon test ICs
- built as a proof of concept
- 80 copies built at one fab
- 80 more copies were built across two lots at a second fab





Test IC Design

Our test IC was designed to allow measurements of multiple distinct manufacturing process variations
- Resistor with 4-wire sensing
  - Metal 1-4, polysilicon, via serpentine, and MOS variations
- Capacitors with integrating oscillator
  - Poly-insulator-poly (PIP) and MOS (gate) variations
- Variations of ring oscillators
  - Nominal, silicon contact (CC), metal 1-2, and polysilicon variations (illustrated below)



We used 10-fold cross-validations and Freund & Schapire's Adaboost M1 method to predict that the presented circuits could classify
- two fabs with up to 98.7% accuracy
- two lots from the second fab with up to 98.8% accuracy

We considered three subsets of the repeated circuits on our test IC:
- **mean** of each circuit type – the best indicator of the underlying manufacturing process variation
- **first 3** of each circuit type – representing the result when only a few copies of each circuit type can be afforded
- **random 3** of each circuit type – like "first 3", but representing a layout of the copies better distributed across the IC
- **all** of each circuit type – representing the raw data from the IC

We present each of our results in the form of a confusion matrices.

Distinguishing two fabs

a	b	← classified as
79	1	a = Lot 2+Lot 3
3	76	b = Lot 1
Correct		97.5%

mean

a	b	← classified as
80	0	a = Lot 2+Lot 3
2	77	b = Lot 1
Correct		98.7%

first 3

a	b	← classified as
765	35	a = Lot 2+Lot 3
35	755	b = Lot 1
Correct		95.6%

random 3

a	b	← classified as
79	1	a = Lot 2+Lot 3
1	78	b = Lot 1
Correct		98.7%

all

Distinguishing two lots from a single fab

a	b	← classified as
40	0	a = Lot 3
1	39	b = Lot 2
Correct		98.8%

mean

a	b	← classified as
38	2	a = Lot 3
1	39	b = Lot 2
Correct		96.2%

first 3

a	b	← classified as
386	14	a = Lot 3
38	362	b = Lot 2
Correct		93.5%

random 3

a	b	← classified as
39	1	a = Lot 3
1	39	b = Lot 2
Correct		97.5%

all

Results

We observe that many of the distributions of measured manufacturing process variation characteristics have little overlap from fab-to-fab and also from lot-to-lot. We apply two metrics to assess the distance between these distributions. We also utilize the intersection between the two estimated probability density functions (PDFs) as a threshold and compute the resulting overlap errors to assess misclassification.

PDF INTERSECTION AND PERCENT CLASSIFIED INCORRECT WHEN THE MEAN OF EACH TYPE OF CIRCUIT IS USED.

Circuit Class	Intersect	Percent Incorrect Lots 2&3	Percent Incorrect Lot 1	Percent Incorrect Average
oscint/cap8_pip	2.19e+07	2.972	4.639	3.805
oscint/cap32_mos_intrin	5.17e+07	7.729	6.246	6.988
oscint/cap32_pip_intrin	5.19e+07	12.970	9.286	11.128
oscint/cap8_mos	1.62e+07	5.052	25.580	15.316
meas_res_blk/pch	1.20e+06	47.095	1.757	24.426
meas_res_blk/nch	1.23e+06	51.369	4.472	27.920
p3/poly1	4.36e+06	2.456	58.485	30.470

Conclusions

We show that it is feasible to reliably identify the fab of origin of an IC by adding special circuits to its design. Based on our analysis, there is no need to distribute the copies of each circuit type across the IC. Furthermore, these circuits could be added with 5% area overhead on a 3mm x 3mm die or 1% on a 7mm x 7mm die.

This experiment used only three lots of ICs from two fabs on a 350nm technology node. Therefore, our results may be the result of chance, and may not extend to other technologies.

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.
SAND2016-xxxx x

U.S. DEPARTMENT OF ENERGY
Sandia National Laboratories