Introduction

Unique IC keys are useful for
- Identification
- Authentication
- Activation/metering
- Encryption

Existing methods
- Depend on EPROMs
- Good for chip ID

Problem with ROM
- Keys can be learned
- ICs can be cloned
- Can program a new chip

Physical Unclonable Functions (PUF)
- Exploit process variation
- $R = f(C)$
- Can't be programmed

Desirable PUF features
- Uniqueness
- Reproducibility
  - Time
  - Environmental var.
- Resistance to
  - Learning
  - Tampering
  - Cloning
- Number of responses exponential to hardware resources
Background

- Proposed PUF methods
  - SRAM power-on patterns
  - Mismatched delay lines / ring oscillators
  - MOS drive current mismatch
  - Leakage currents

- Subject to environmental variations
  - Ex: The effect of ambient temperature on
    - FET saturation current is quadratic
    - RO freq. (path delay) is linear
    - Leakage current is exponential
Background

- **Passive** structures are less sensitive to temperature variations than **active** devices
  - Environmental var. → bad for reproducibility
  - Process var. → good for diversity

We exploit **variations** in the **metal resistivity** of the power grid. Advantages:

- **Linear** function of temperature
- Utilize a large **existing** passive resource
  - Minimizes overhead

We define a PUF in **two** ways

1. **Voltage** drops across power distribution system
   - Subject to effects of active devices
2. Equivalent **resistances** (voltage divided by global current)
   - Eliminates variations caused by active devices
Chip Design and PUF Circuit

- Manufactured in 65nm IBM tech.
- Power grid has six C4 Power Ports (PP)
- Stimulus/Measure Circuits (SMC)
  - Inserted below each PP
  - Small footprint (50 µm²)
  - A ‘shorting inverter’
  - A ‘voltage sense transistor’
- Method requires a voltage sense pin
- External instrumentation
  - Voltmeter
  - Global current meter
PUF Circuit Internals

IBM 65 nm test chips

Power ports

Power grid

Scan chain

FF inverter chain

SMC circuit

10-layer power grid

Sense

Inverter

Voltmeter

Globally-routed
Two PUF Definitions

- Clocks are shut down on other circuits
- The leakage current is calibrated out
- Shorting inverter stimulates the power grid
- Produces a measurable voltage drop
- In voltage-only PUF, the voltage drop is used directly
- In equivalent resistance PUF, $R_{eq}$ can be found using voltage division

$R_{eq} = \frac{0.9 - V_{sense}}{I_{glob}}$

$V_{drop} \approx 10\text{mV}$

$V_{sense} \approx 10\text{mV}$

$I_{glob} \approx 1\text{mA}$
PUF Response Procedure

For SMC1
- **Shorting inverter** and **voltage sense** transistor switched on
- Voltage sense wire is measured w.r.t. ground
- **Sense voltage** is subtracted from **power supply voltage**
- **Global current** is also measured

This is repeated for the other 5 SMCs

We have the 6 voltage drops for the first PUF

The **equivalent resistances** (Ω) are computed by dividing the **voltage drop** (V) by the **global current** (A)

These six voltages and resistances constitute a 6-dimensional voltage and resistance signature

We conducted experiments on **36 chips**

We also obtained a **noise/control sample** by repeating the procedure on one chip 12 times over a 6-hour period
Voltage Drop Signature Visualization

Ordering is unique, so actual dispersion is greater. Note dispersion of chip data: magn. between and within.

Control data relatively stable.

Each chip has 6 voltages in its column.

5 3 3 3 5 2 4 4 3 1 0 3
1 4 5 0 1 3 1 0 5 4 3 0
2 2 4 1 2 0 3 5 0 5 2 5
0 5 0 4 4 4 5 1 2 0 4 1
4 1 1 5 0 5 2 3 1 3 1 2
3 0 2 2 3 1 0 2 4 2 5 4
Equiv. Resistance Signature Visualization

Results similar to volt. drop

Less variation due to cancelled effect of FETs
Signature Aliasing

- We want to estimate the probability of aliasing
  - i.e., two chips produce the same signature

- We define the aliasing *probability* w.r.t. the *uncertainty* (noise) in our measurements
  - The noise floor we found was significantly greater than the precision of our instruments
  - Characterize the chip and control samples separately to establish a SNR
  - Use an upper bound on the noise to define the lower limit of our ability to distinguish signatures

- Define the distance between two signatures using the Euclidean distance
  - Reduces multi-dim. space to single dimension
Using the Euclidean Distance

Consider the resistances for chip 1 and chip 2

- Combine these into a 6-dim. vector
- The chips can be represented as points in 6-dim. space
- We can compare the positions in this 6-dim. space using the Euclidean distance
- Using the noise data, we effectively establish a sphere around each of these points
- This allows us to be prudent about the uncertainty of the position

Then we can define the probability of aliasing as

- The probability that any chip distance is less than the radius of the sphere

\[ R_{C1} = <9.7, 9.6, 9.9, 8.8, 8.9, 10.2> \]
\[ R_{C2} = <7.9, 8.1, 8.7, 8.9, 8.3, 8.1> \]
\[ D = ||R_{C1} - R_{C2}|| = 3.36 \]
Probabilistic Analysis

- Use all pairs of chip distances ($n$ choose 2) to build a **distance histogram**
  - There are 630 pairs for 36 chips
  - Best fit with a **Gamma** distribution

- Repeat same procedure for the noise sample

- Use the **noise PDF** to estimate the Eucl. distance that **upper bounds** 99.7% of noise distances ($3\sigma$)
  - Provides a practical upper limit on the magnitude of noise

- Estimate the **fraction** of chip **distances** less than this threshold using the **chip PDF**
  - Represents fraction of chip distances that are too close to reliably distinguish
  - This **yields** the **probability of aliasing**
  - None of the chip signatures we encountered were closer than this threshold
Noise Data Histogram and Fit

# Occurrences

0 75 8 152 227 303

Euclidean Distance (Ohms)

- 0.00 0.02 0.04 0.06 0.08 0.10 0.12

0 3 6 9 15 21 27

Probability Density

0.1
Chip Data Histogram and Gamma Fit

Min. chip dist. is 5X the max. noise dist.
Chip vs. Control Distributions

Probability of aliasing

Chi² PDF
Control PDF
Chip PDF

# Occurrences

Euclidean Distance (Ohms)

Probability Density

0.1 0.3 0.4 0.5

0 1 2 3 4 5

0 9 27 45 63 81
Results of Signature Diversity

For both **voltage** and equiv. **resistance** PUFs:
- Chip **dispersion** was **much greater** than that of the noise data
  - Distances more than 40X greater on average

Using this procedure, the probability of aliasing is
- Equiv. Resistance: $6.9 \times 10^{-8}$ or 1 in 15 million
- Voltage only: $3.5 \times 10^{-11}$ or 1 in 28 billion

Added dispersion in Voltage signatures due to env./proc. variations of MOS devices

Since we didn’t monitor/control temperature precisely, we prefer to use the equiv. resistance PUF

Only 6 SMCs were used
- Results could improve significantly with more
Future Work

- Beyond the single-on tests
- Results
- How can this PUF be applied
- An integrated architecture
An Exponential Number of Challenges

- PUFs ideally have $2^n$ responses
  - where $n =$ number of SMCs
  - We’ve only shown 6 challenge/response pairs

- Can short at multiple locations simultaneously
  - Can observe voltage at each short location

- Number of meaningful challenges given by
  $$\sum_{i=1}^{n} i \binom{n}{i} = n \cdot 2^{n-1}$$

- For example, with $n =$ 6 SMC's
  - There are 192 are challenges
An Exponential Number of Challenges

<table>
<thead>
<tr>
<th>Singles</th>
<th>Pairs</th>
<th>Triplets</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Singles" /></td>
<td><img src="image2.png" alt="Pairs" /></td>
<td><img src="image3.png" alt="Triplets" /></td>
<td><img src="image4.png" alt="All" /></td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\text{Total} & = n2^{n-1} \\
\text{n} & = \text{...} \\
2 \binom{n}{2} & = \text{...} \\
3 \binom{n}{3} & = \text{...} \\
\end{align*}
\]
Effect of Adding Additional Tests

- Beyond the paper, we considered incrementally adding the multiple-on tests
  - One-ons, two-ons, up to six-on
  - Dim. of the signature: 6, 36, 96, 156, 186 and 192
- Probability of aliasing decreases significantly
  - Saturates at the five-on tests
- Same power grid resistances are being exercised
  - Superposition could apply and then additional tests wouldn't add to the signature diversity
  - However, we divide each voltage drop by the global current, which is the sum of multiple stimulus currents
Cumulative Aliasing Probabilities

Factors of increase 36X the separation
Different Application Scenarios

- Ensuring trust, from wafer to board
  - Perform challenge before and after delivery
  - E.g. voting machines, critical installations
  - High-precision instruments
  - Global current can be measured
  - Method we have shown can be applied

- In an embedded application
  - E.g. cryptography, hardware metering
  - Measuring global current is impractical
  - Difficult to build an on-chip voltmeter
  - We propose utilizing spatial differences in voltage within M1
A Fully-Integrated Architecture

Two M1 voltages are sensed simultaneously.

A controller handles generating responses given a challenge.

OpAmp

Compares voltages to produce a 1 or 0.

Scan data and clock

1 bit of digital signature

A controller handles generating responses given a challenge.

A controller handles generating responses given a challenge.

A controller handles generating responses given a challenge.
Questions?

Thanks for listening!