A Powerless and Non-volatile Counterfeit IC Detection Sensor in a Standard Logic Process Based on an Exposed Floating-Gate Array

Muging Liu and Chris H. Kim

University of Minnesota, Minneapolis, MN
liux3300@umn.edu
Outline

- Motivation
- Proposed counterfeit IC detection sensor
- 0.35µm test chip measurement results
- Summary
Outline

• Motivation
  • Proposed counterfeit IC detection sensor
  • 0.35µm test chip measurement results
• Summary
Internet of Things (IoT) and Security

Smart industry
Smart home
Smart vehicle
Smart city

Fake devices
Fake servers
Hackers
Eaves-dropping

Source: Infineon
Counterfeit Types

More than 80% of counterfeits

- Recycled
- Remarked
- Overproduced
- Defective
- Cloned
- Tampered
- Forged Documentation

Electronics Counterfeiting Threat

1. E-Waste
2. Counterfeit PC Parts
3. Counterfeit Military Parts
4. Counterfeit Automotive Electronics

- Desolder, sort, clean
- Electronics Supply Chain
Counterfeit IC Detection

**Physical Inspection**
- Straightforward method
- Costly and time consuming
- An expert required to interpret the test results
- Invasive, destructive

**Electrical Test**
- Verify functionality and performance
- Measure the usage time of the chip
- Cannot detect physical attacks

**X-ray Imaging**
- Source: Honeywell

**IC Recycling Sensor**

3.6cm 3.4cm
Outline

• Motivation

• Proposed counterfeit IC detection sensor

• 0.35µm test chip measurement results

• Summary
Eflash with Exposed Floating Gate

Humidity, chemicals, debris, electrostatic charges, physical contact, etc.

- Expose floating gate (FG) to the environment.
- Non-volatile and powerless.
- No process overhead, no back-end processing.
Counterfeit IC Detection Scheme

- $\Delta_{\text{normal}}$ should account for drift and retention loss under normal conditions.
Logic Compatible Embedded Flash

- No process overhead, logic-compatible
- Floating gate formed by back-to-back gates.
- Higher coupling ratio reduces write voltage.

Coupling device  Program/Read device  Erase device

S. H. Song, et al., JSSC, May 2013
Logic Compatible Embedded Flash

- Coupling ratio determined by the sizing ratio between M1 and M2/3.

Coupling ratio (CR) = N/(N+1)

S. H. Song, et al., JSSC, May 2013
• Erase and program mechanism: Fowler-Nordheim (FN) tunneling.
16x16 Eflash Based Sensor Array
Sensor Configuration and Die Photo

CR = 0.98, CR = 0.99, CR = 0.99, CR = 0.99
1X Read 1X Read 2X Read 4X Read

20µm X 20µm opening (4 rows)
20µm X 40µm opening (4 rows)
20µm X 60µm opening (4 rows)
40µm X 40µm opening (4 rows)

Exposed sensor Unexposed sensor

1.23mm
1.57mm

VCO Readout & Column Buffers
High Voltage Switch
16 x 16 Eflash Sensor Array
Outline

• Motivation
• Proposed counterfeit IC detection sensor
• 0.35µm test chip measurement results
• Summary
Initial Frequency Characterization

- Negligible frequency difference/drift between consecutive samples
- Higher coupling ratio (CR), larger transistors → more efficient erase/program.
Retention Characteristics

- Robust retention characteristics if not tampered.
Temperature Attack Results

- Alternate rows are erased/programmed for better charge collection.
- Frequency change occurs in programmed cells.
Humidity Attack Results

- Alternate rows are erased/programmed for better charge collection.
- Frequency change occurs in programmed cells.
Temperature vs. Humidity Attack

- Smaller frequency shift in unexposed cells for both type of attacks
Particle/Debris Attack Results

Debris lands on exposed FG

Before

After

Exposed cells • Unexposed cells

\[ \Delta f \times 10^4 \]
Summary

• A powerless and non-volatile eflash based counterfeit IC detection sensor demonstrated

• 0.35µm test chip measurement results
  – Temperature attack.
  – Humidity attack.
  – Particles/debris attack.