

MECCA : A Robust Low-Overhead PUF using Embedded Memory Array

Aswin Raghav Krishna*, Seetharam Narasimhan, Xinmu Wang and Swarup Bhunia

Department of Electrical Engineering and Computer Science *Case Western Reserve University* Cleveland, Ohio, USA

Statement of Acknowledgement: This presentation was made possible, in part, through financial support from the School of Graduate Studies at Case Western Reserve University



Outline

- Introduction
 - Security challenges
- Background and Motivation
 - Existing PUFs
 - Motivation for a new PUF
- MECCA PUF
 - Overview
 - Characterization
 - Methodology
- Results
- Conclusion



Introduction

NewEgg sells 300 counterfeit Core i7-920 CPUs, KIRFers pump their fists

By Darren Murph 🖾 posted March 7th 2010 6:28PM

Finally, here's the statement Intel just sent us, explaining in no uncertain terms that these are counterfeit parts:

"Intel has been made aware of a limited number of counterfeit i7 920 packages in the marketplace, specifically Newegg, and is working to how many and/or where they are being sold. The examples we have seen are not Intel products but are counterfeits. Buyers should contact their place of purchase for a replacement and/or should contact their local law enforcement agency if the place of purchase refuses to help.

Intel is getting samples to inspect and until then we can say that everything in the package appears fake. Some of the photos of the processor look like it is a casting and not even a real processor of any kind. Newegg has moved quickly to replace the suspect units."

Counterfeit products in the news

Fake chips from China threaten U.S. military systems

Published 9 September 2010

🚼 Share | 🖂 😭 唑 🛅 | 🔤 Email to a friend

Defense Department has become a prime target for counterfeiters, most of them Chinese companies; from November 2007 through May 2010, U.S. Customs officials said they seized 5.6 million bogus chips -- yet many more are finding their way into the United States and even the military

Apple cracks down on counterfeit products sold in NYC, files lawsuit against Queens vendors

By Amar Toor 🖾 posted Aug 19th 2011 4:45AM

There may be more than a few fake Apple Stores in China, but for the moment, Cupertino's anti-KIRF crusade seems focused squarely on New York City. According to *Reuters*, Apple has filed a trademark infringement lawsuit against two stores in Queens, alleging that they sold unauthorized cases, headphones and other accessories for the iPhone, iPad and iPod. In the complaint, the company claims that the products in question were all emblazoned with its familiar fruit logo, along with the phrase, "Designed by Apple in California. Assembled in China." The suit also demands that one of the stores, called Apple Story (seriously), change its name to avoid confusion with the real retail outlet and that both vendors disclose full lists of people who both supplied and purchased the goods.



CHFS 2011









Introduction



- Traditional approach
 - Store digital key in NVM, e.g. EEPROM
 - Problems
 - Subject to invasive attacks
 - Protection against invasive attacks is very expensive
 - Higher fabrication costs

Physical Unclonable Functions (PUFs)



- Intrinsic process variations manifested as device parameter variations
- Convert parameter variations to digital responses



- Why PUFs?
 - Highly Secure
 - Volatile no stored keys
 - Unpredictable
 - Large challenge response set
 - Low cost variation is inherent





Examples of PUFs



RO PUF -Suh *et al, 2007*



SRAM PUF -Guajardo *et al*, Holcomb *et al* 2007



Arbiter PUF -Lee et al, 2004



Butterfly PUF -Kumar *et al,* 2008





MECCA PUF - Motivation

- Why do we need a dedicated circuit for a PUF⁷
 - Can PUF be an added functionality of an existing circuit?
- Memory is a great choice
 - A significant portion of ASICs and SOCs is occupied by SRAM memory
- SRAM PUF Each cell produces only one bit
- How to extract multiple responses from memory array?
 - MECCA PUF: <u>MEmory Cell Characterization</u> based <u>Authentication PUF</u>





MECCA PUF



Failure mechanisms in an SRAM cell

Write failure: Unsuccessful write with wordline activation

- Access failure: Insufficient differential voltage failures developed during a read operation
- Read failure: Flipping of the data during read
- Hold failure: Leakage currents in cell cause data destruction with low supply voltage

Static

Temporal





Effect of word line duration on write-ability



 $WL_3 > WL_2 > WL_1$



- Consists of a string of inverters with outputs of g subgroups of inverters connected to a g X I mux
- Core SRAM array remains unaltered
 - Only the qualified write signal is modified
- $P_{0,} P_{1,...} P_{n}$ becomes part of the challenge
 - Extract multiple responses from a given set of cells

Methodology



• **Response generation:**

- Choose address of *r*-cells $\{A_0, A_1, \dots, A_r\}$
- Perform background write known initialization state
 - For each cell, Mem[A_i]=k; k={0,1}
- Write to cells with reduced wordline duration using programmable delay circuit

• $C = \{A_0, ..., A_r, P_0, ..., P_n\}$

• Read out *r*-bit response from cells $\{Y_0, Y_1, ..., Y_r\}$



Simulation framework

- Monte Carlo simulations under both inter-die $(\sigma = 10\%)$ and intra-die $(\sigma = 6\%)$ variations
- Predictive Technology Model (PTM) 45nm
- r = 128 bit response; m = 1000 chips; k = 3 WL durations
- The WL durations are obtained from the distribution of write times required for all cells
- Mean WL of delay circuit is chosen as mean write time of all cells
 - other 2 WLs are obtained based on an accepted distribution of 1s and 0s in the response







- Uniqueness/Security: Show that different PUFs generate different responses
 - Inter die response analysis: How many bits are different between any two PUF responses

$$HD_{Inter-die} = \frac{2}{m^*(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^m HD_{perc}(m_i, m_j)$$







- Average inter-die HD is close to 50% at mean WL
- But...
- Reduces by a max of 2.5% for other WLs Why??







- **Reliability:** How good is a PUF at generating the same response consistently
 - Intra die response analysis: How many bits are different between two responses from the same PUF

$$HD_{Intra-die} = \frac{1}{S} \sum_{k=1}^{S} HD_{perc}(R_i, R_{i,k})$$



PUF more stable with temperature fluctuations than supply voltage fluctuations!!!



 \geq



Ageing analysis

- Ageing Temporal variations in the device parameters due to degradation of transistors
 - Particularly bad in PMOS transistors due to high negative fields at high temperatures



BTI = Bias Temperature Instability

- > Why bother?
 - Can affect reliability!!





- Estimate degradation over lifetime several models available
- Monte Carlo simulations with estimated degradation to obtain a guard band around each WL duration
- > Classify cells falling within guard band as unreliable



- At mean WL, upto 8 bits are unstable due to ageing!
- Solutions
- Disregard unreliable cells (bits) from response generation
- If # bits is less, maybe it can be tolerated



Summary



- A memory cell based PUF called MECCA PUF using write failures
 - Dual functionality PUF and data storage
 - Extract multiple responses from a memory array
 - Good uniqueness and reliability of responses
 - Scalable with relative increase in die-to-die and within-die process variations in nanoscale technologies
- Future work
 - Hardware validation
 - Modeling attacks

Thank You

0

Questions ??