Enter search terms:
Search
in this series
Advanced Search

Notify me via email or RSS

Browse

Collections
Disciplines
Authors

Author Corner

Author FAQ

Links

University Libraries
UMass Amherst
Contact Us

Masters Theses 1896 - February 2014

On-Chip True Random Number Generation in Nanometer CMOS

Download

SHARE

Vikram Belur Suresh, *University of Massachusetts - Amherst*

Follow

Document Type
Open Access

Degree Program
Electrical & Computer Engineering

Degree Type
Master of Science in Electrical and Computer Engineering (M.S.E.C.E.)

Year Degree Awarded
2012

Month Degree Awarded
February

Keywords
True Random Number Generation, Process Variation, Circuit calibration

Abstract

On-chip True Random Number Generator (TRNG) forms an integral part of a number of cryptographic systems in multi-core processors, communication networks and RFID. TRNG provides random keys, device id and seed for Pseudo Random Number Generators (PRNG). These circuits, harnessing physical random variations like thermal noise or stray electromagnetic waves are ideally expected to generate random bits with very high entropy and zero correlation. But, progression to advance semiconductor manufacturing processes has brought about various challenges in the design of TRNG. Increasing variations in the fabrication process and the sensitivity of transistors to operating conditions like temperature and supply voltage have significant effect on the efficiency of TRNG designed in sub-micron technologies. Poorly designed random number generators also provide an avenue for attackers to break the security of a cryptographic system. Process variation and operating conditions may be used as effective tools of attack against TRNG. This work makes a comprehensive study of the effect of process variation on metastability-based TRNG designed in deep sub-micron technology. Furthermore, the effect of operating temperature and the supply voltage on the performance of TRNG is also analyzed. To mitigate these issues we study entropy extraction mechanisms based both on algorithmic approach and circuit tuning and compare these techniques based on their tolerance to process variation and the energy overhead for correction. We combine the two v approaches to efficiently perform self-calibration, using a hybrid of algorithmic correction and circuit tuning to compensate the effect of variations. The proposed technique provides a fair trade-off between the degree of entropy extraction and the overhead in terms of area and energy, introducing minimal correlation in the output of the TRNG. Besides the study of the effect of process variation and operating conditions on the TRNG, we also propose to study the possible attack models on a TRNG. Finally, we propose a probabilistic approach to design and analysis of TRNG using a stochastic model of the circuit operation and incorporating the random source in thermal noise. All analysis is done for 45nm technology using the NCSU PDK transistor models. The simulation platform is developed using HSPICE and a Perl based automation flow.

Advisor(s) or Committee Chair

BURLESON, WAYNE P