Analysis of On-Chip True Random Number Generators based on Power Supply Variation

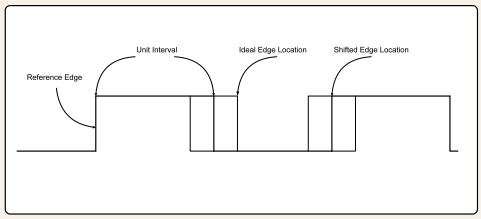
Wayne Burleson, Salma Mirza

INTRODUCTION

Implementation of True Random Number Generators is crucial to the strength of most cryptographic applications. As computational capacity of RFIDs increases, they may be able to implement public key cryptosystems. This would require efficient generation of truly random keys which are also resilient to malicious attack.

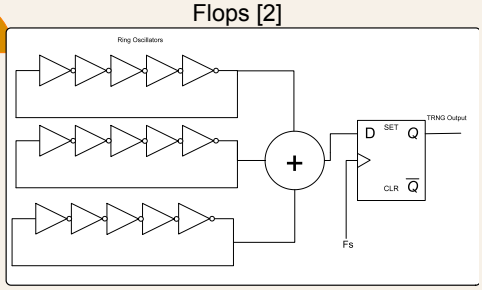
JITTER

Jitter: Temporal Uncertainty in Arrival time of a Signal



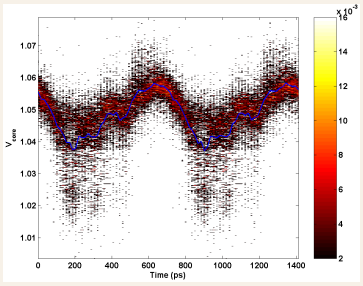
This uncertainty is harvested in the design of True Random Number Generators

Example: TRNGs using uncertainty in periods of Ring Oscillators [1], Creating set-up time violations to create metastability in in D-Flip Flops [2]



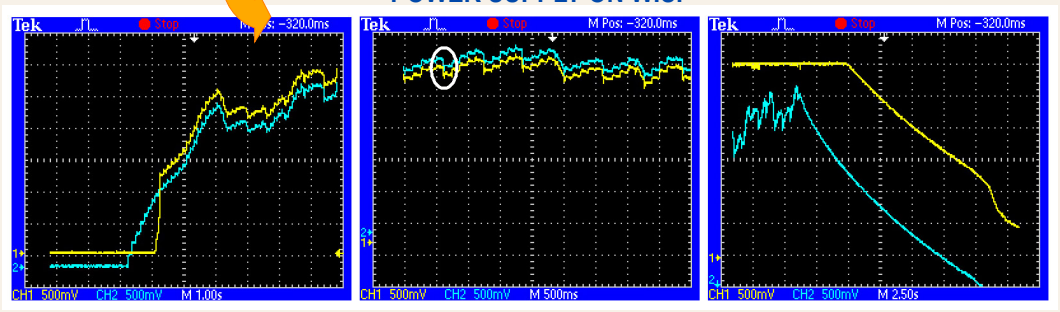
POWER SUPPLY NOISE

"Power supply noise is Cyclostationary [3]"



At the same point in each cycle noise statistics are the same

POWER SUPPLY ON WISP



READ BEGINS TAG ID BEING TRANSMITTED READ ENDS

Regulated Power Supply ----- Unregulated Power Supply

The power supply on the WISP follows a definite pattern and is predictable

References:
[1] B. Sunar, W. J. Martin, D. R. Stinson, **A Provably Secure True Random Number Generator with Built-in Tolerance to Active Attacks**, IEEE Transactions on Computers, vol 58, no 1, pages 109-119, January 2007
[2] Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, **Fast True Random Generator in FPGAs**
[3] T. Fischer *et. al.*, "A 90nm Variable-Frequency Clock System for a Power-Managed Itanium®-Family Processor," *ISSCC 2005.*