ECE 459/559
Secure & Trustworthy Computer Hardware Design

True Random Number Generators

Garrett S. Rose

Spring 2017

THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

Random Numbers in Cryptography

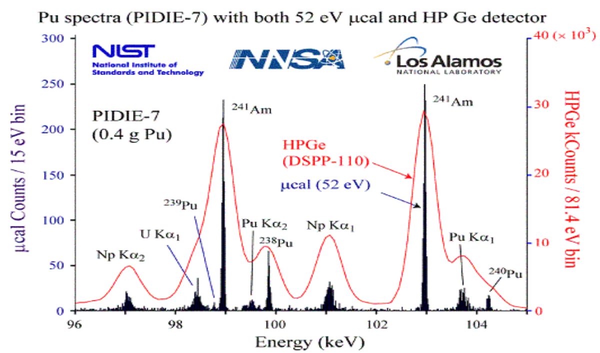
- The keystream in a one-time pad
- The secret key in DES encryption
- The prime numbers p, q in the RSA encryption
- The private key in digital signal algorithm (DSA)
- The initialization vectors used in many ciphers

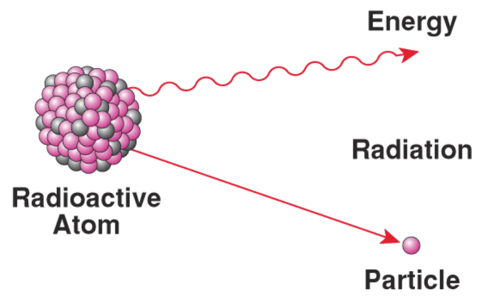
Pseudo-Random Number Generator

- Pseudo-Random Number Generator (PRNG) – A polynomial-time function f(x) that expands a short random string x into a long string f(x) that *appears* random
- Not truly random in that:
  - Deterministic algorithm
  - Dependent on initial values (seed)
- Objectives:
  - Fast
  - Secure

True-Random Number Generator (TRNG) Sources

- Only truly random number sources are those related to physical phenomena such as rate of radioactive decay of an element or thermal noise of a semiconductor





- True randomness bound to natural phenomena
- Impossible to algorithmically generate truly random numbers

Good TRNG Design

- Entropy source:
  - Randomness present in physical processes
  - Examples: thermal and shot noise in circuits, brownian motion, nuclear decay
- Harvesting mechanism:
  - Mechanism shouldn't disturb the physical process but collects as much entropy as possible
- Post-processing (optional):
  - Apply to mask imperfections in entropy sources or harvesting mechanism to provide tolerance in presense of environmental changes and tampering

Sunar et al., “A Provably Secure True Random Number Generator,” IEEE TCOMP 2007.

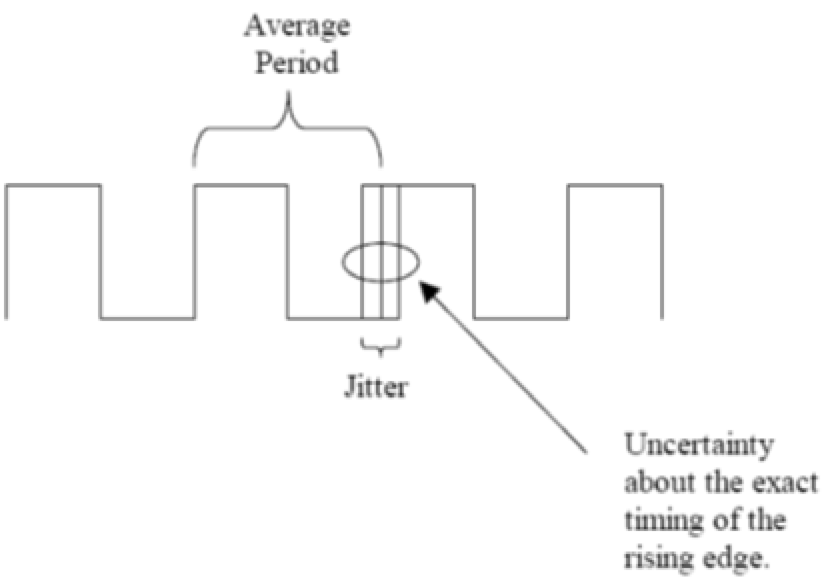
Set of Requirements

- Sunar et al. advocate for purely digital TRNG design
- Harvesting mechanism should be simple
  - Unpredictability of TRNG shouldn't be based on complexity of harvesting mechanism
  - Unpredictability solely based on entropy source
- No correction circuits are allowed
- Compact and efficient design (high throughput per area and energy consumed)
- Simplicity of design should sufficient to allow rigorous analysis

Sunar et al., "A Provably Secure True Random Number Generator," IEEE TCOMP 2007.

Example Method: Clock Jitter

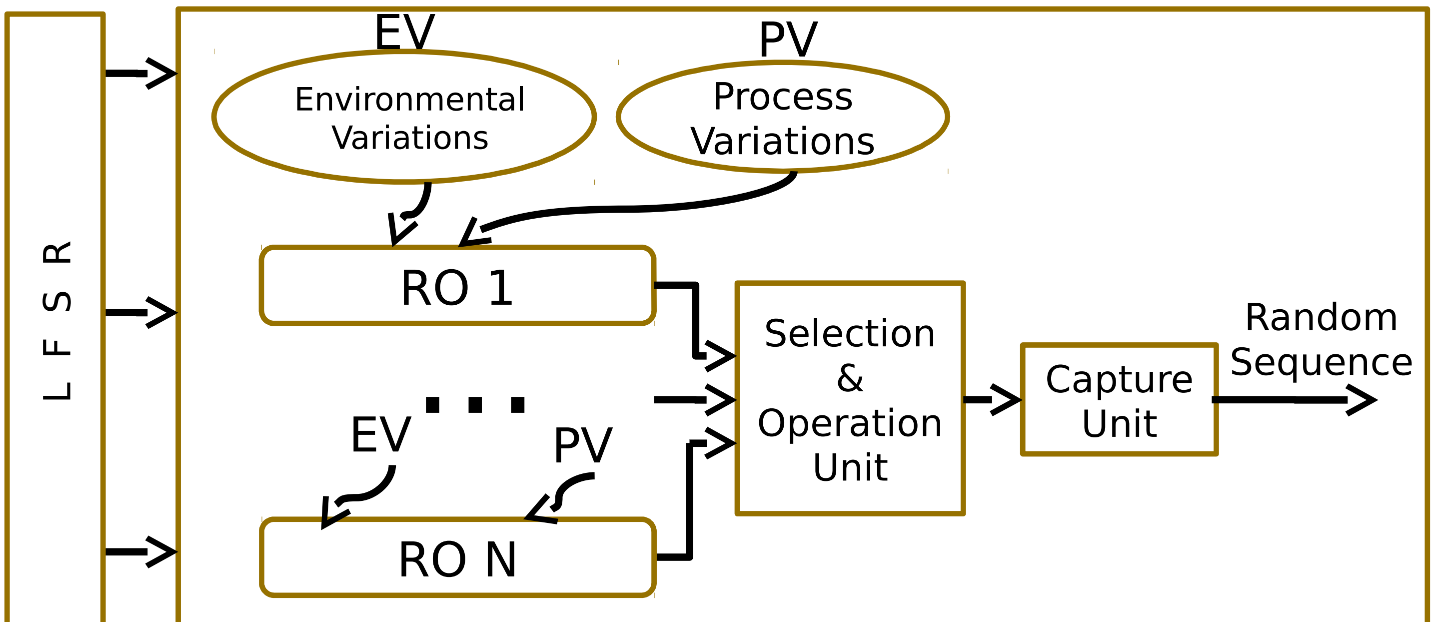
- Jitter is variation in the significant transitions of a clock
- Jitter is non-deterministic (random)
- Sources of jitter:
  - Semiconductor noise
  - Cross-talk
  - Power supply variations
  - Electromagnetic fields



THE UNIVERSITY OF TENNESSEE KNOXVILLE

An Example TRNG Structure

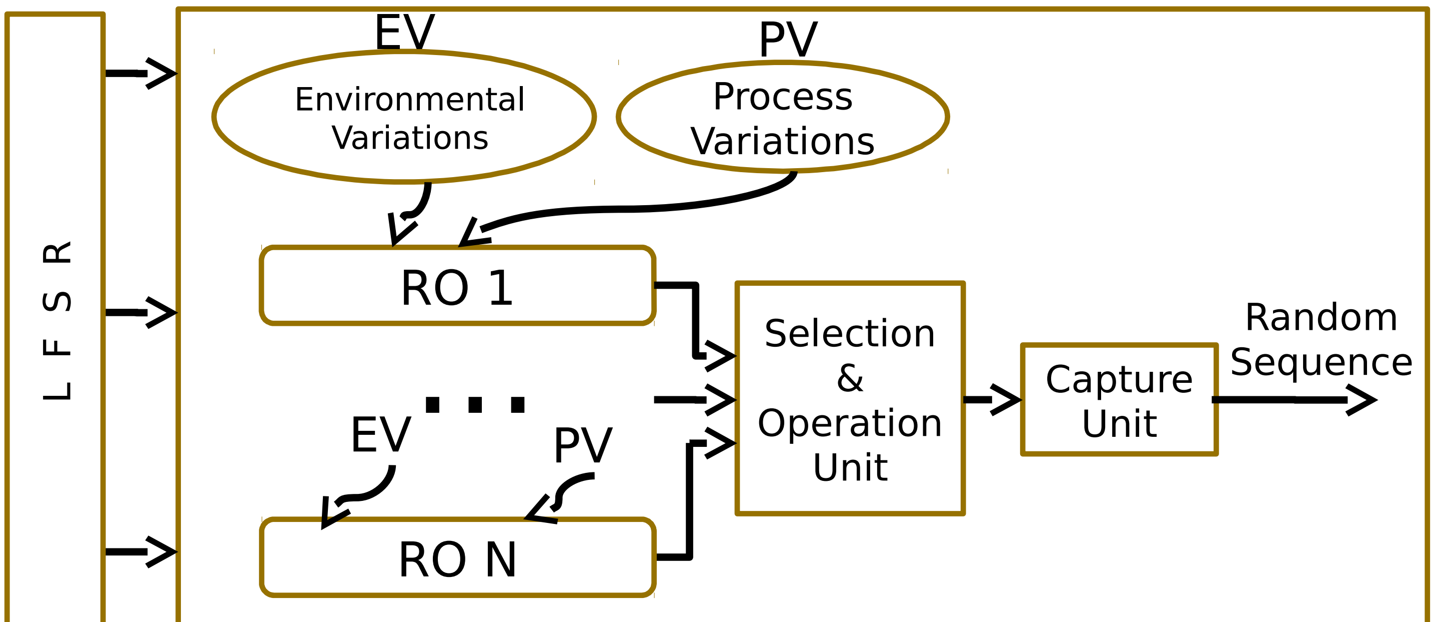
- LFSR: Generate random patterns, causing random noise
- The LFSR “seeds” the TRNG



LFSR = Linear Feedback Shift Register

An Example TRNG Structure

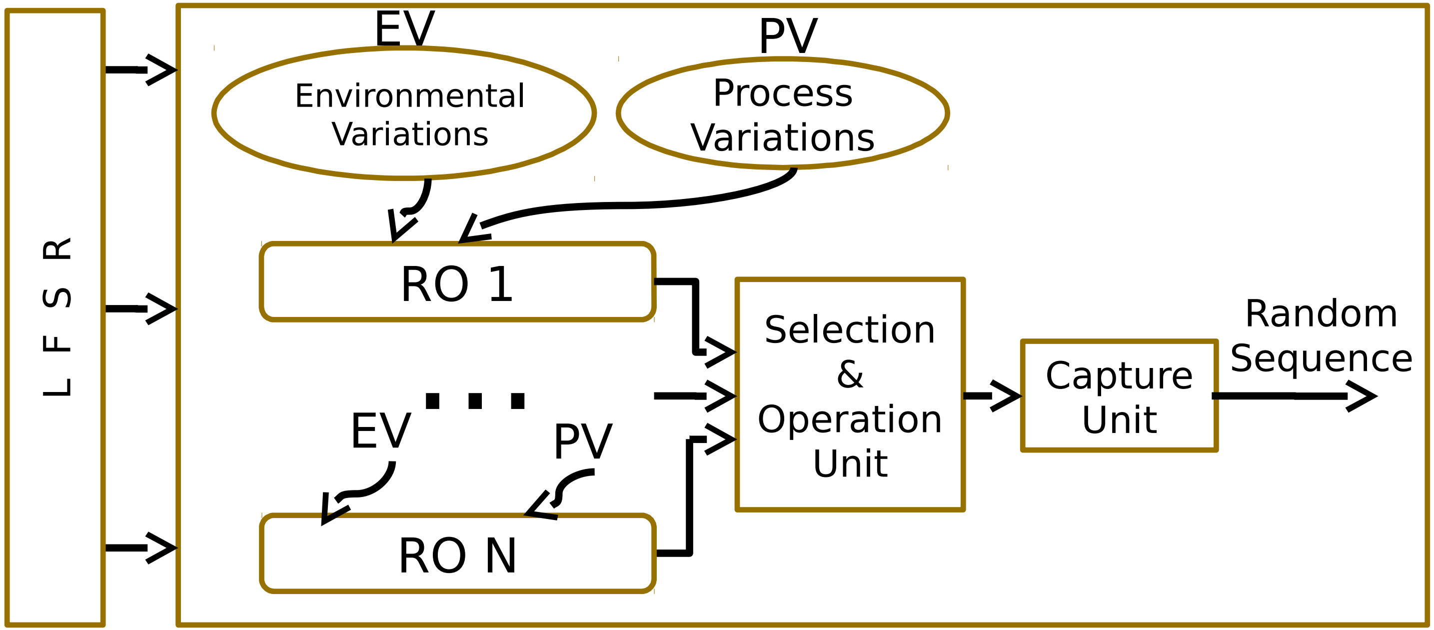
- Ring Oscillators – Provide process variations & environmental variations; also random phase jitter



LFSR = Linear Feedback Shift Register

An Example TRNG Structure

- Selection & Operation Unit – Translates random phase of ROs into digital; could use XOR operation

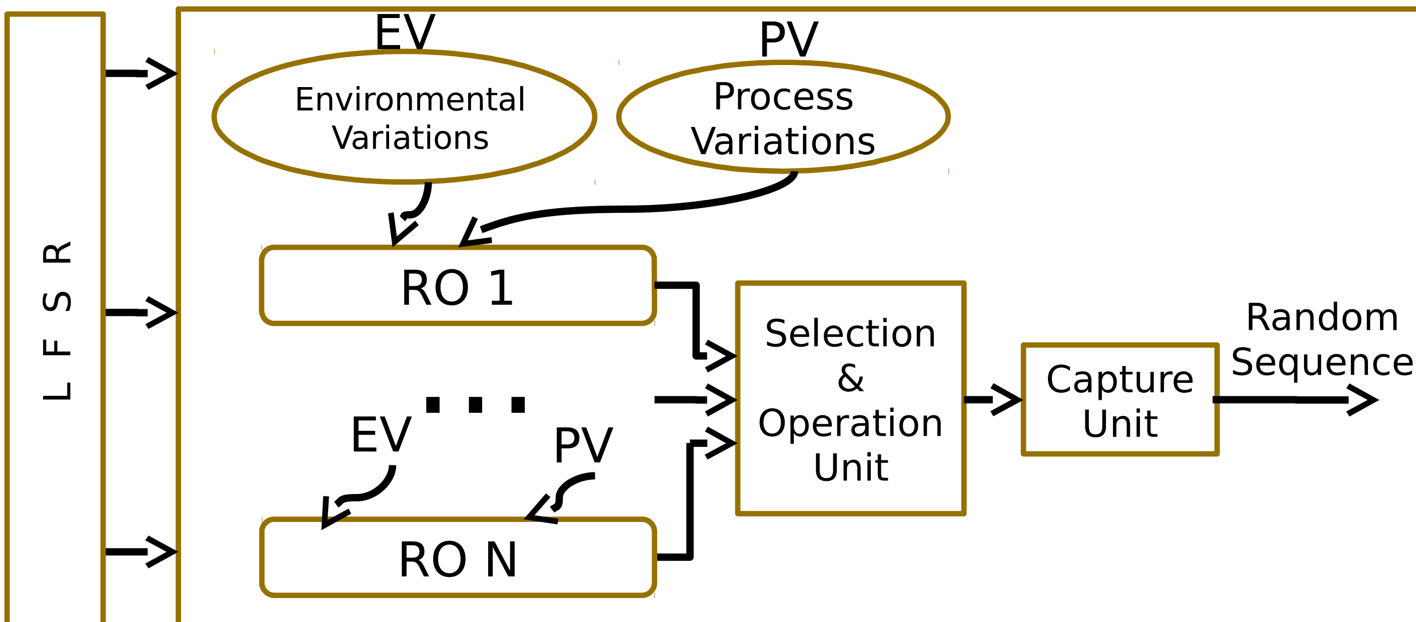


THE UNIVERSITY OF TENNESSEE KNOXVILLE

LFSR = Linear Feedback Shift Register

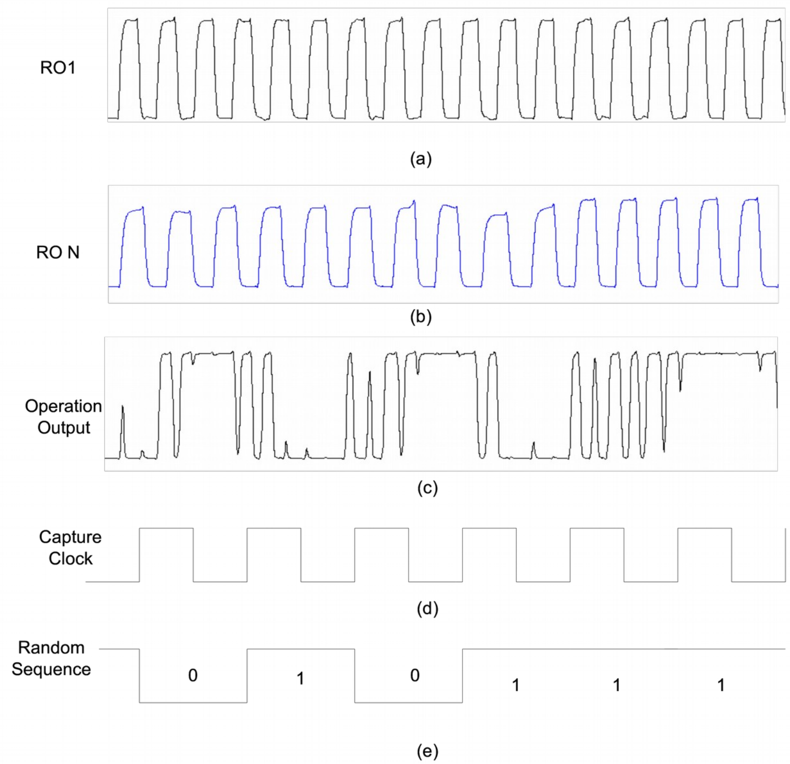
An Example TRNG Structure

- Capture Unit – Make sure digital value sampled with frequency of required true random number



LFSR = Linear Feedback Shift Register

Example TRNG Output



THE UNIVERSITY OF TENNESSEE KNOXVILLE