True Random Number Generator

Random Numbers in Cryptography

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

Pseudo-random Number Generator

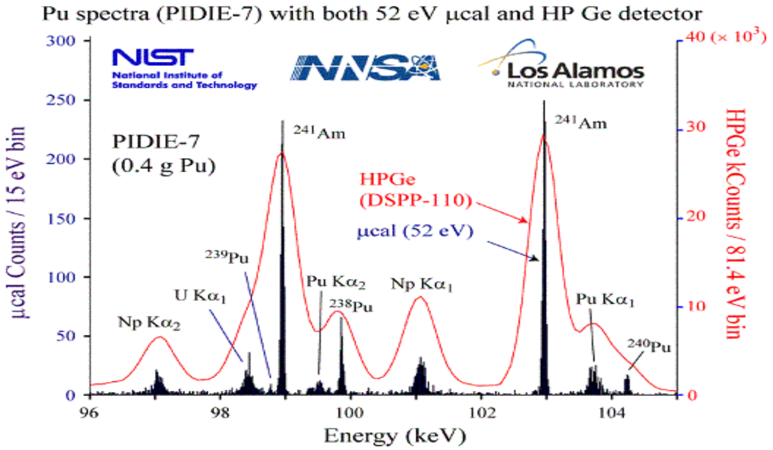
- **Pseudo-random number generator:**
  - A polynomial-time computable function f (x) that expands a short random string x into a long string f (x) that appears random

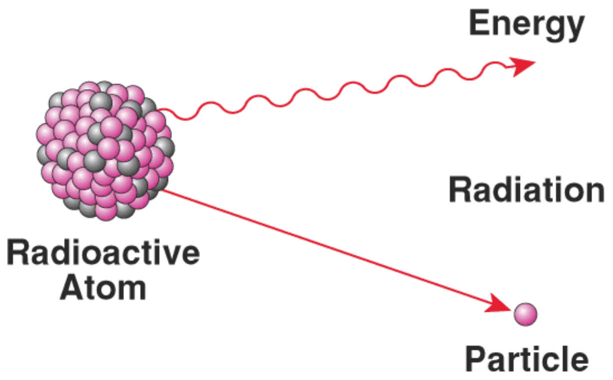
- **Not truly random in that:**
  - Deterministic algorithm
  - Dependent on initial values (seed)

- **Objectives**
  - Fast
  - Secure

Sources

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





- Randomness is bound to natural phenomena. It is impossible to algorithmically generate truly random numbers.

Good TRNG Design

- **Entropy Source:**
  - Randomness present in physical processes such as thermal and shot noise in circuits, brownian motion, or nuclear decay.
    - **Shot noise**, the time-dependent fluctuations in electrical current caused by the discreteness of the electron charge, is well known to occur in solid-state devices
- **Harvesting Mechanism:**
  - The mechanism that does not disturb the physical process but collects as much entropy as possible.
- **Post-Processing (optional):**
  - Applied to mask imperfections in entropy sources or harvesting mechanism or to provide tolerance in the presence of environmental changes and tampering.

Good TRNG Design

- **Entropy Source:** The source, from which we generate TRNG, for harvesting randomness present in physical processes such as Brownian motion thermal and shot noise in circuit or nuclear decay. Entropy source must provide randomness and it is the most critical. Biasness should be eliminated in the collection or post-processing steps.
- **Harvesting Mechanism:** Several harvesting mechanisms have been proposed. The mechanism should not disturb the physical system but collects as much entropy as possible. The harvesting mechanism should be simple. The unpredictability of the TRNG should not be based on the complexity of the harvesting mechanism, but only on the unpredictability of the entropy source. The design should be compact and efficient.
- **Post Processing:** This component is not needed in all designs. A post-processor is applied to mask, if needed, imperfections in entropy source or harvesting mechanism

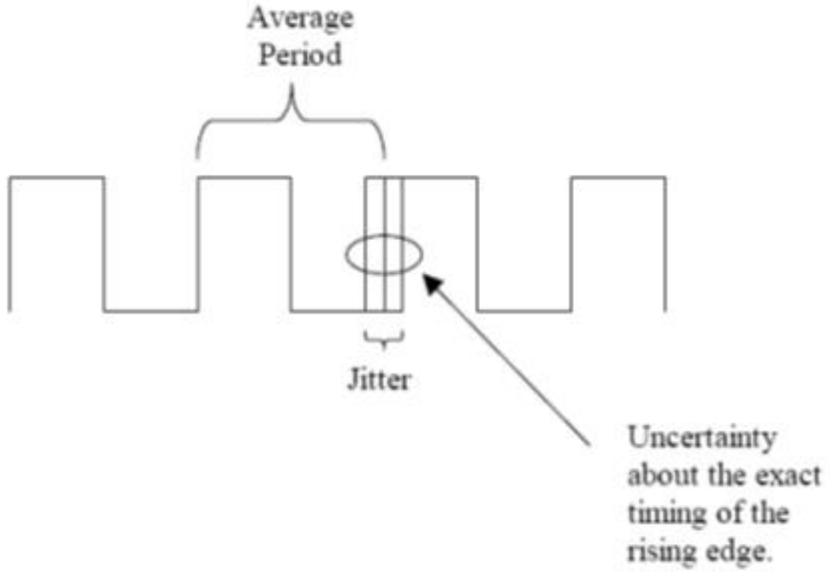
Set of Requirements

- The Design Should be purely digital
- The harvesting mechanism should be simple.
  - The unpredictability of the TRNG should not be based on the complexity of the harvesting mechanism, but only on the unpredictability of the entropy source.
- No correction circuits are allowed
- Compact and efficient design (high throughput per area and energy spent).
- The design should be sufficiently simple to allow rigorous analysis.

Method : Clock Jitter

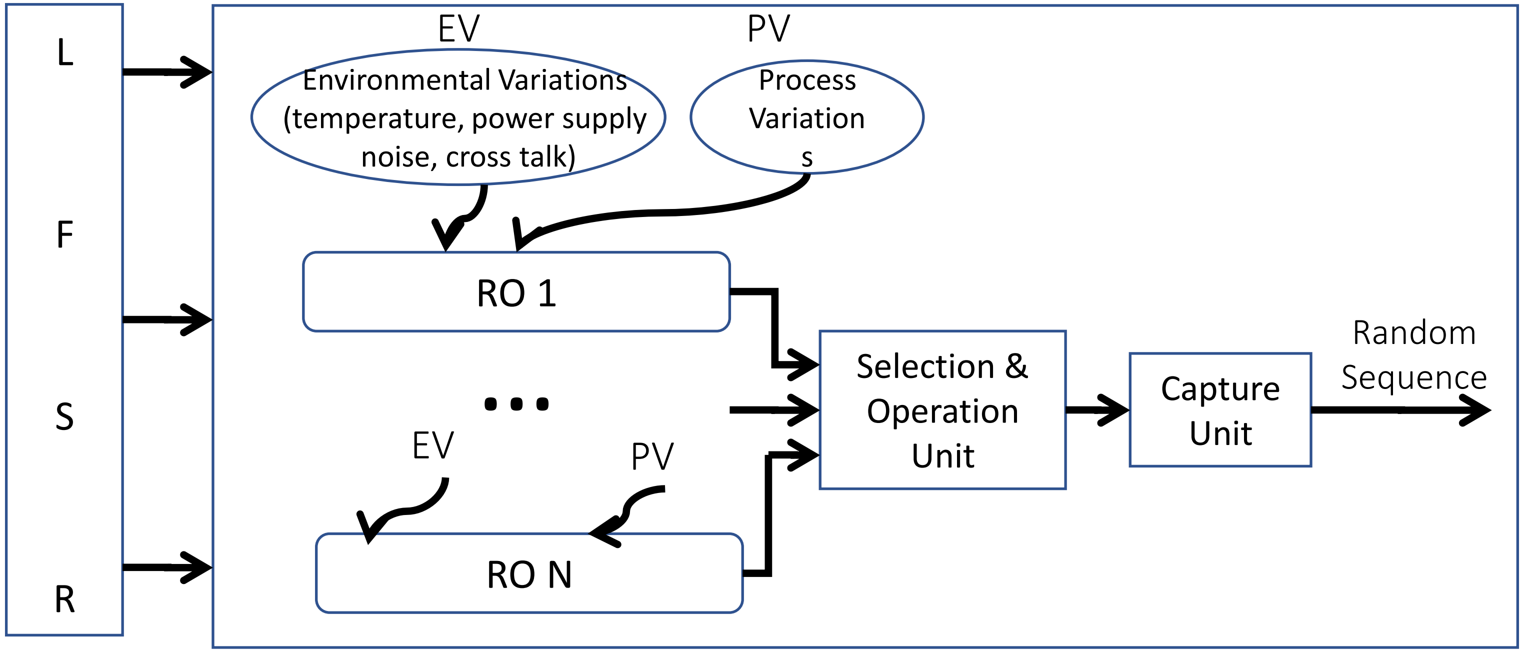
- Jitter is variations in the significant instants of a clock
- Jitter is nondeterministic (random)

- **Sources of Jitter:**
    - Semiconductor noise
    - Cross-talk
    - Power supply variations
    - Electromagnetic fields



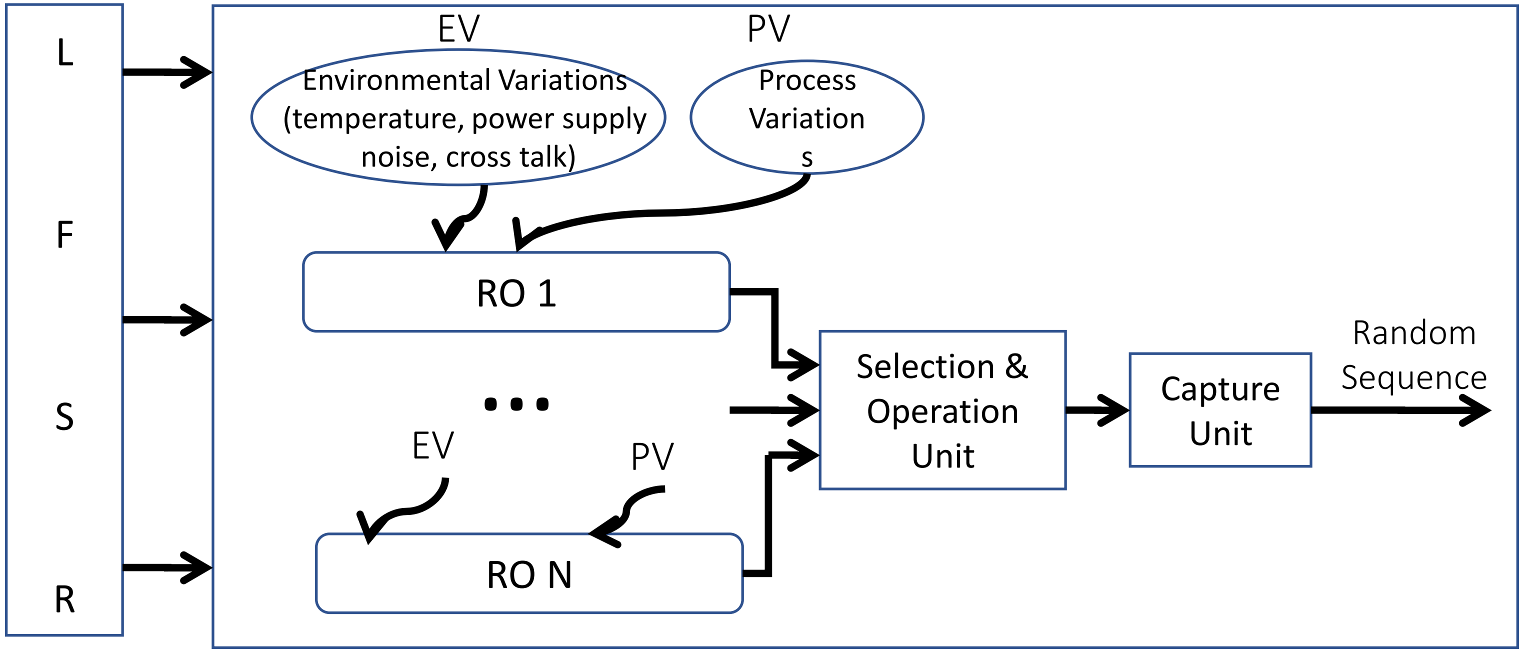
TRNG Structure

- **LFSR**: Generate random patterns, causing random switching noise.
- A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. It generates random patterns causing random switching noise. This provides environmental variations. The environmental variations and process variations make the entropy source more random.


L
F
S
R
EV
PV
Environmental Variations (temperature, power supply noise, cross talk)
Process Variation s
RO 1
...
EV
PV
RO N
Selection & Operation Unit
Capture Unit
Random Sequence

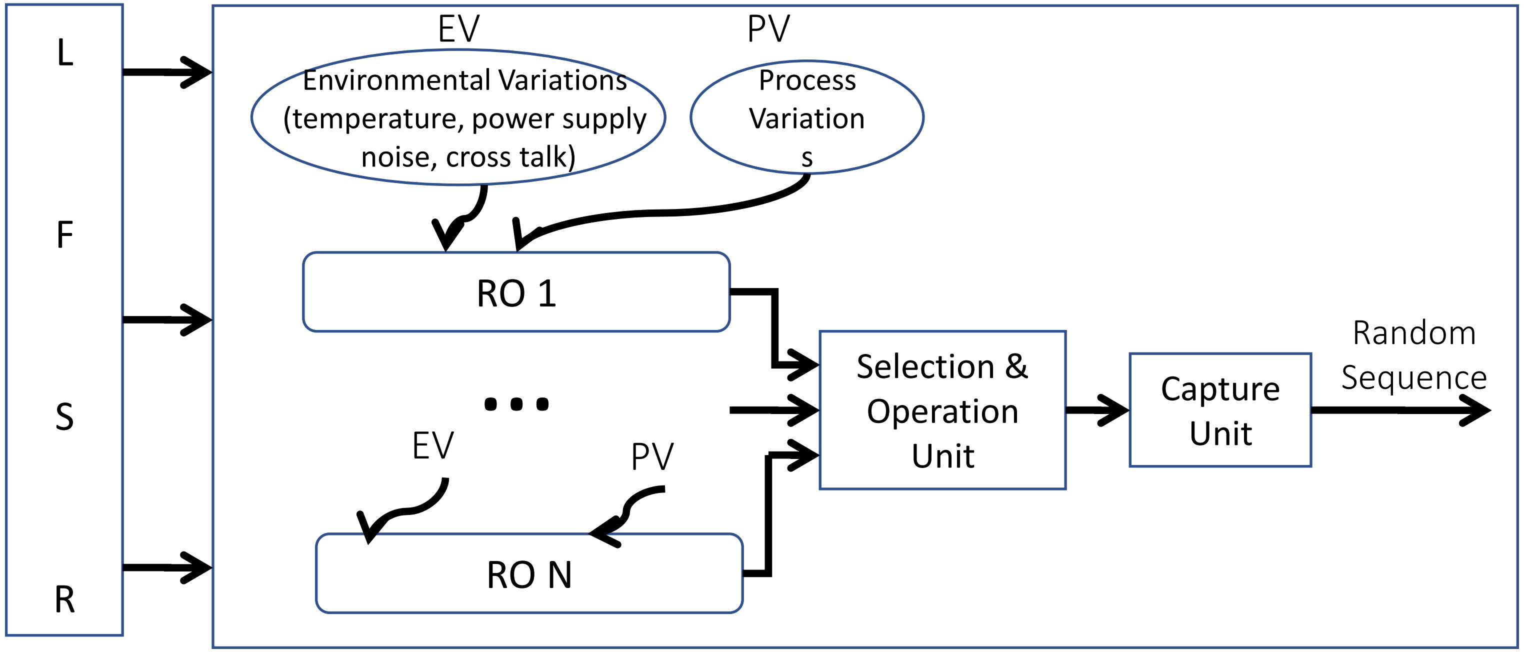
TRNG Structure

- **Ring Oscillators**
    - Process variations & environmental variations
    - Random phase jitter


L
F
S
R
EV
PV
Environmental Variations (temperature, power supply noise, cross talk)
Process Variation s
RO 1
...
EV
PV
RO N
Selection & Operation Unit
Capture Unit
Random Sequence

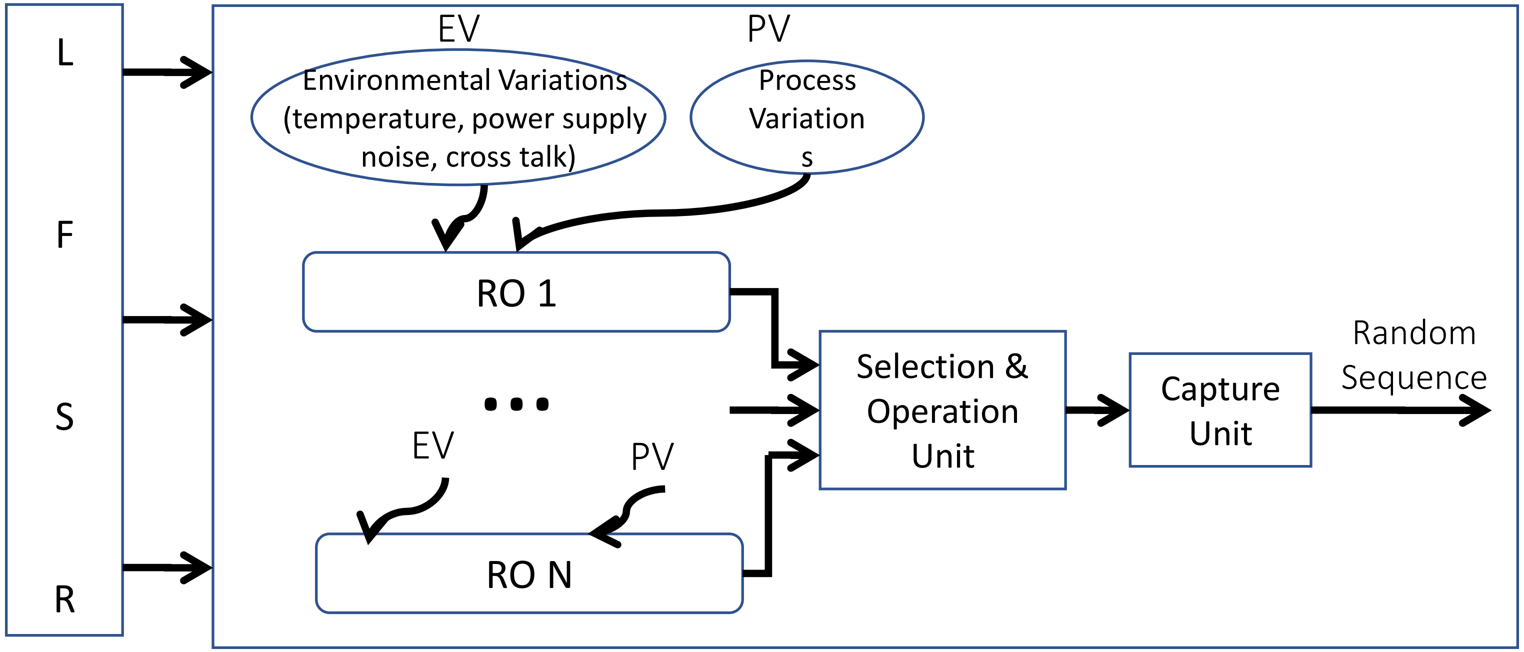
TRNG Structure

- **Selection & Operation Unit:** The random phase of ring oscillators could be translated into digital values by this unit, such as XOR operation

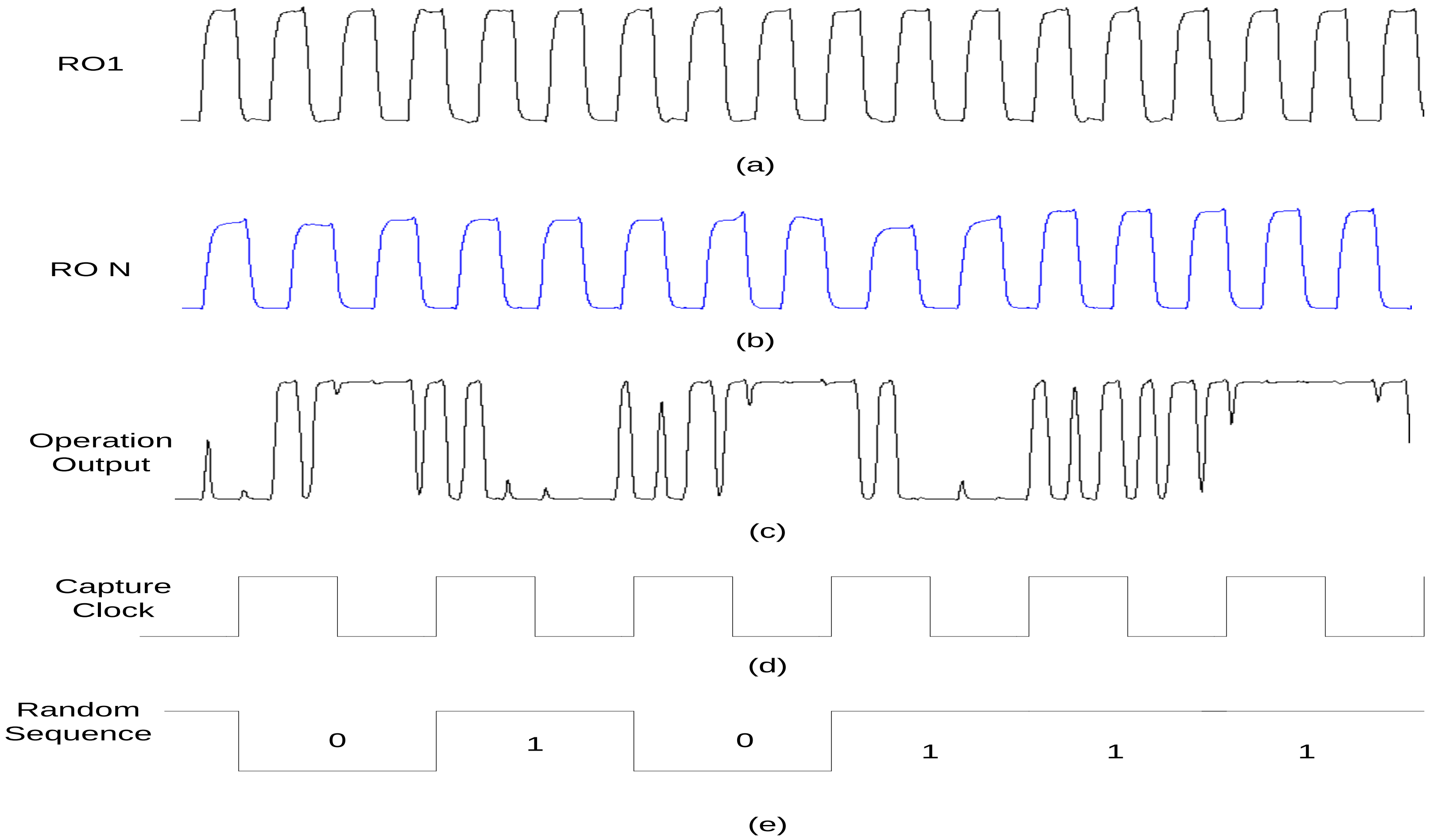

L
F
S
R
EV
PV
Environmental Variations (temperature, power supply noise, cross talk)
Process Variation s
RO 1
...
EV
PV
RO N
Selection & Operation Unit
Capture Unit
Random Sequence

TRNG Structure

- **Capture Unit:** Make sure the digital value is sampled with the frequency of the required true random number.


L
F
S
R
EV
PV
Environmental Variations (temperature, power supply noise, cross talk)
Process Variation s
RO 1
...
EV
PV
RO N
Selection & Operation Unit
Capture Unit
Random Sequence

TRNG Output


RO1
(a)
RO N
(b)
Operation Output
(c)
Capture Clock
(d)
Random Sequence
0
1
0
1
1
1
(e)