07 Truly Random Number Generators (TRNGs)

Engr 399/599: Hardware Security

Grant Skipper, PhD.
Indiana University

Adapted from: Mark Tehranipoor of University of Florida

Agenda

- Review PUFs
- Start & Finish TRNG
- Reminder Project Extension! -> This Friday! 2/21/24 Midnight!
- P2 Assigned Monday!

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

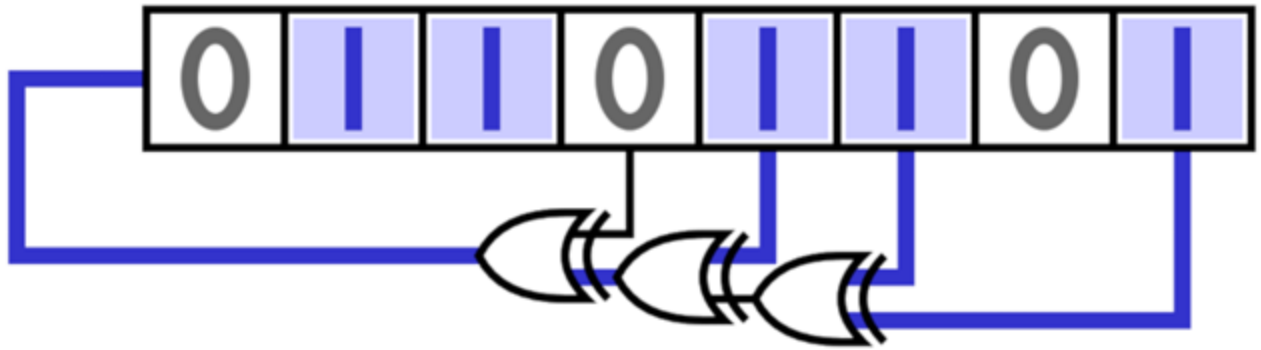
- **Pseudo-random number generator:**
  - A polynomial-time computable function f (x) that expands a short random string x into a long string f (x) that appears random

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

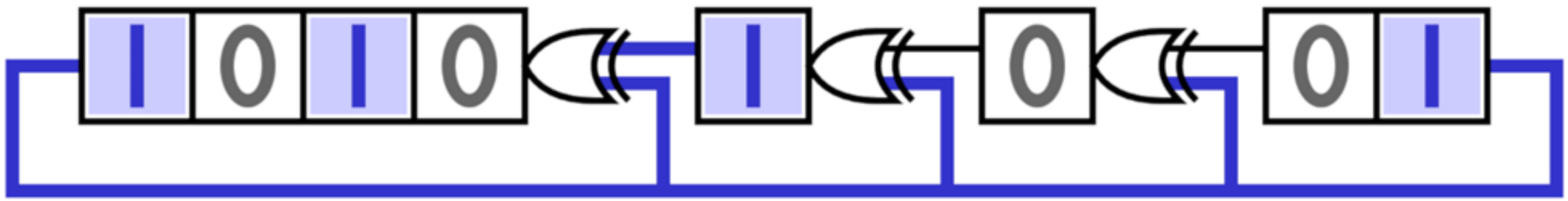
Mersenne Twister (Pokemon)
LFSR (lazy cryptography)

- **Objectives**
  - Fast
  - Secure

Linear Feedback Shift Register

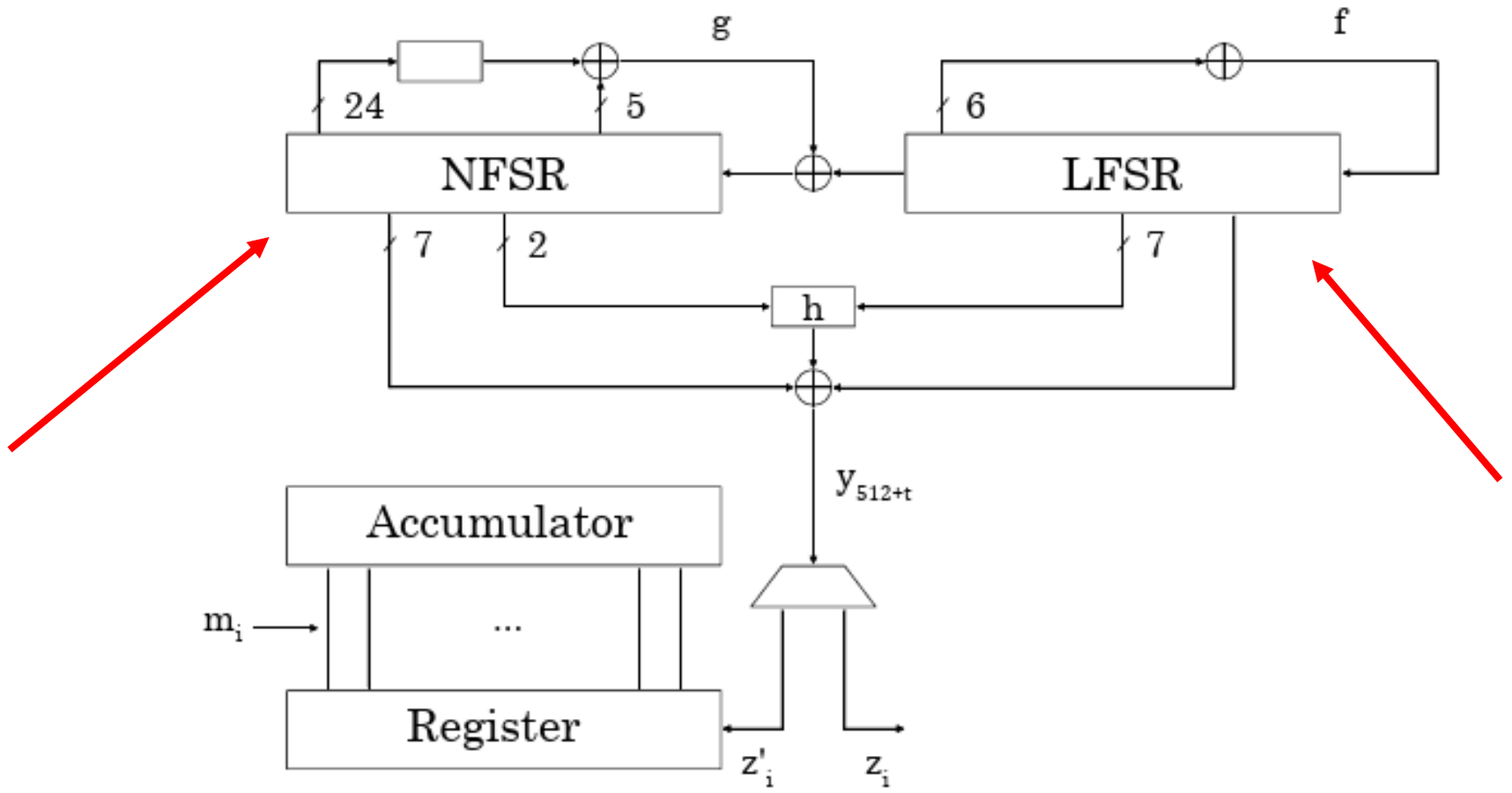


Fibonacci Configuration LFSR



Galois Configuration LFSR

LFSRs Still Used?

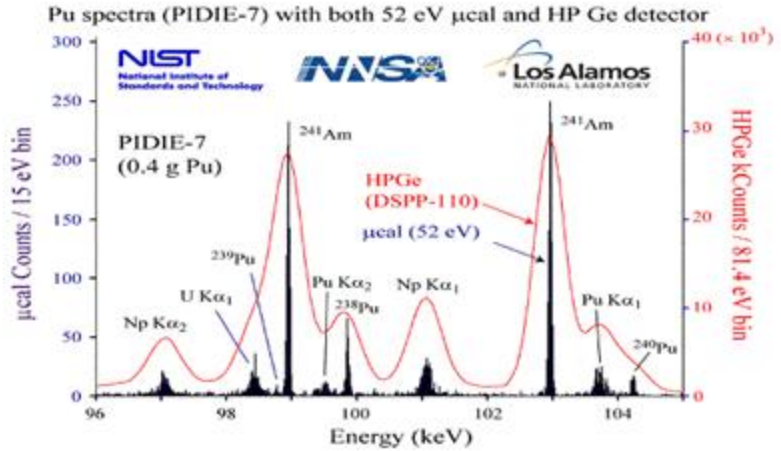


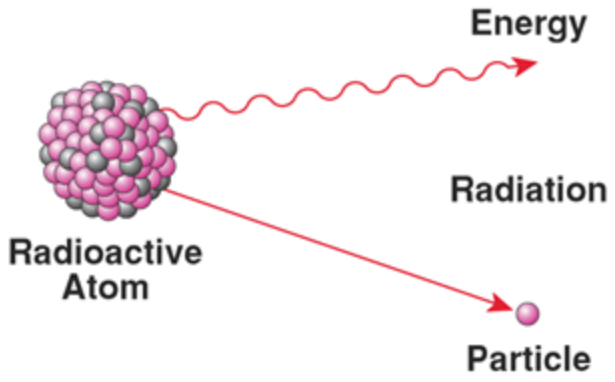
NIST LWC Grain128-AEAD (2021)

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.

Lavarand!!!





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

Microcalorimeter (black) and high-purity germanium (red) spectra of a mixture of plutonium isotopes. Minimal thermal noise is achieved at 100 mK. High sensitivity is due to use of a superconducting quantum interference device.

https://www.aps.org/units/fps/newsletters/2006/july/article6.html

Good TRNG Design

- **Entropy Source:**
  - Randomness present in physical processes such as thermal and shot noise in circuits, brownian motion, or nuclear decay.
- **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.

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.

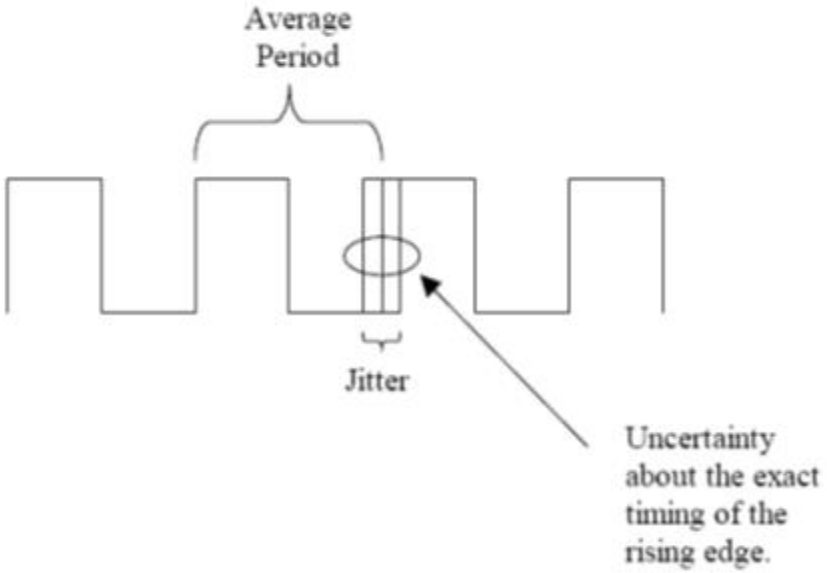
Set of Requirements

- 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

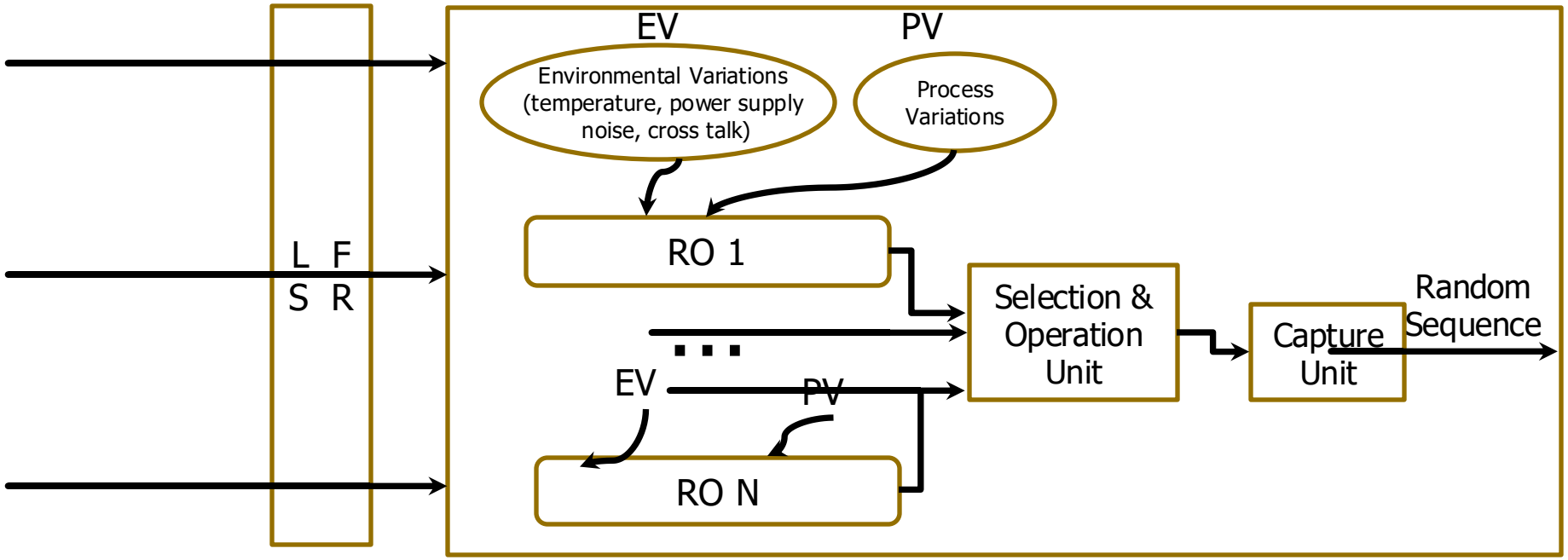
- Jitter is variations in the significant instants of a clock
- Jitter is nondeterministic (random)

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



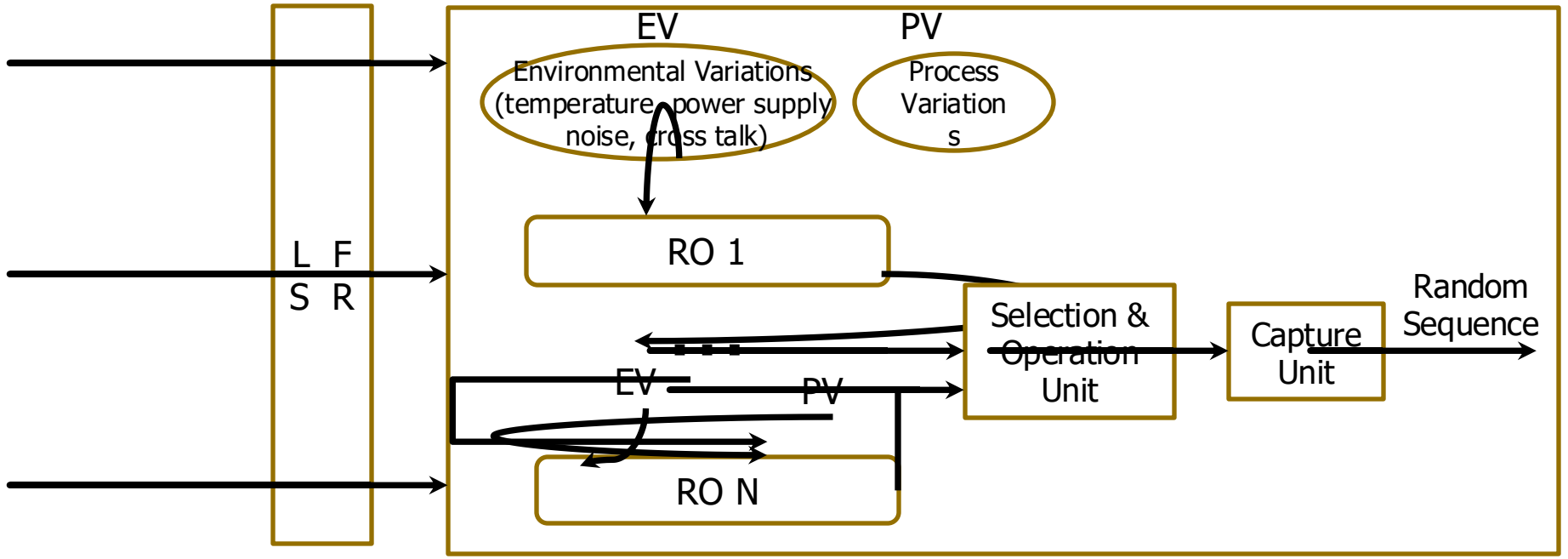
TRNG Structure

- **LFSR**: Generate random patterns, causing random switching noise



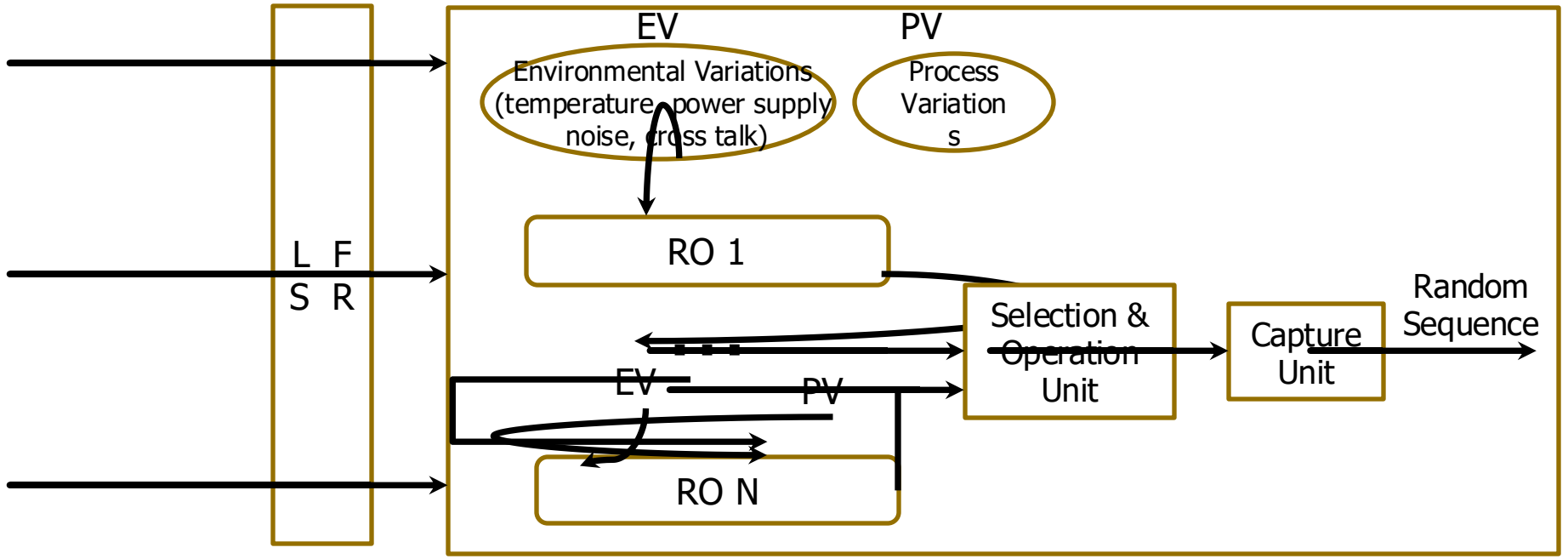
TRNG Structure

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



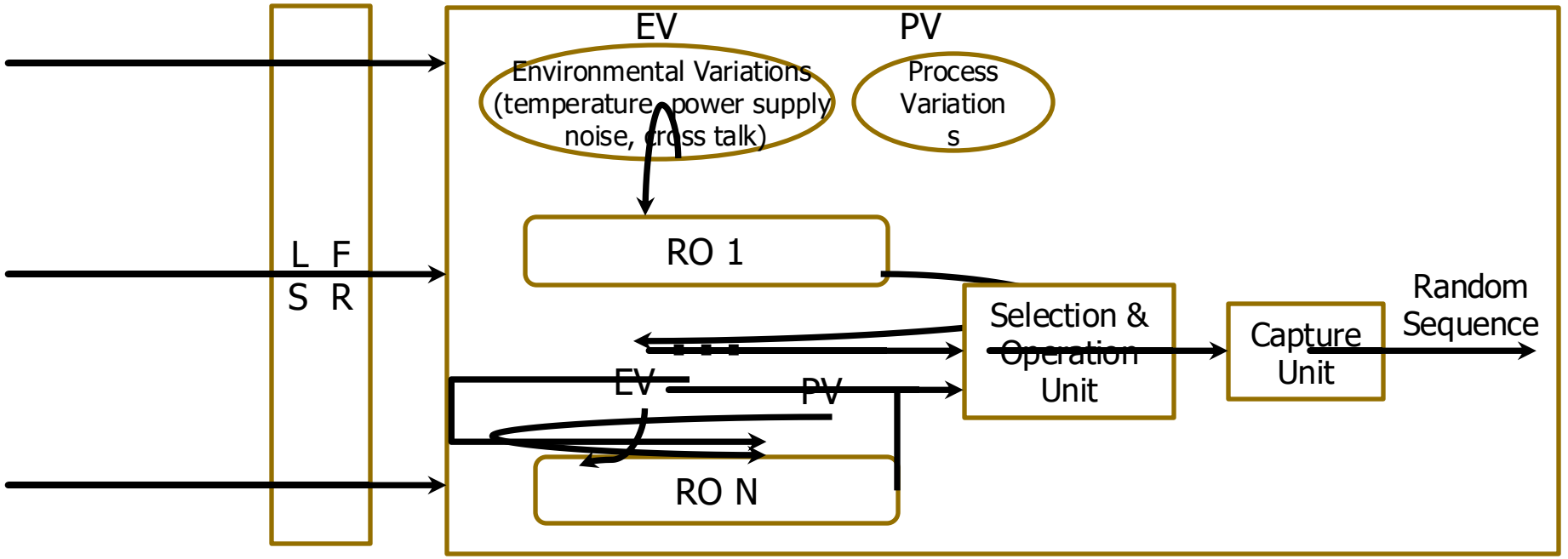
TRNG Structure

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

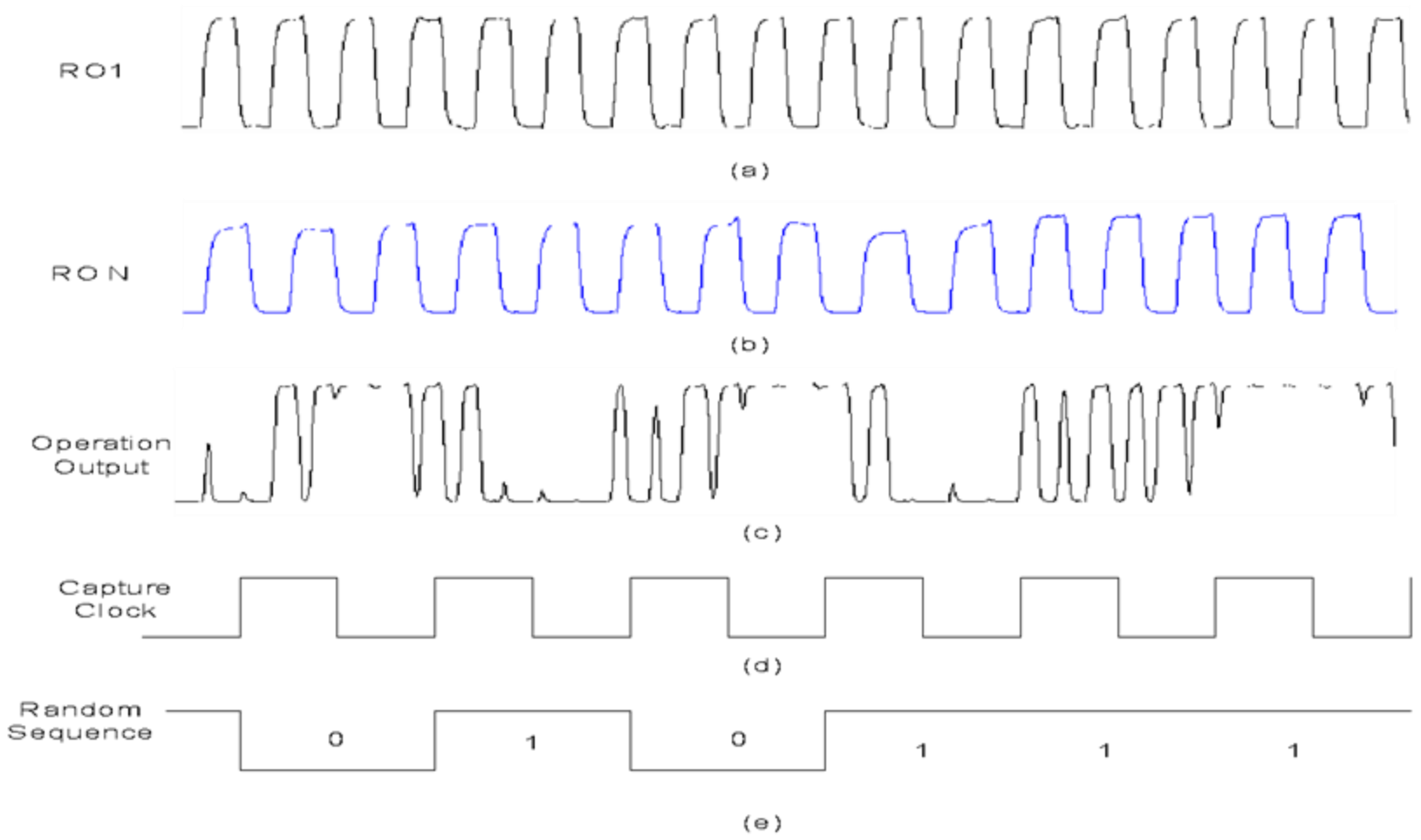


TRNG Structure

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



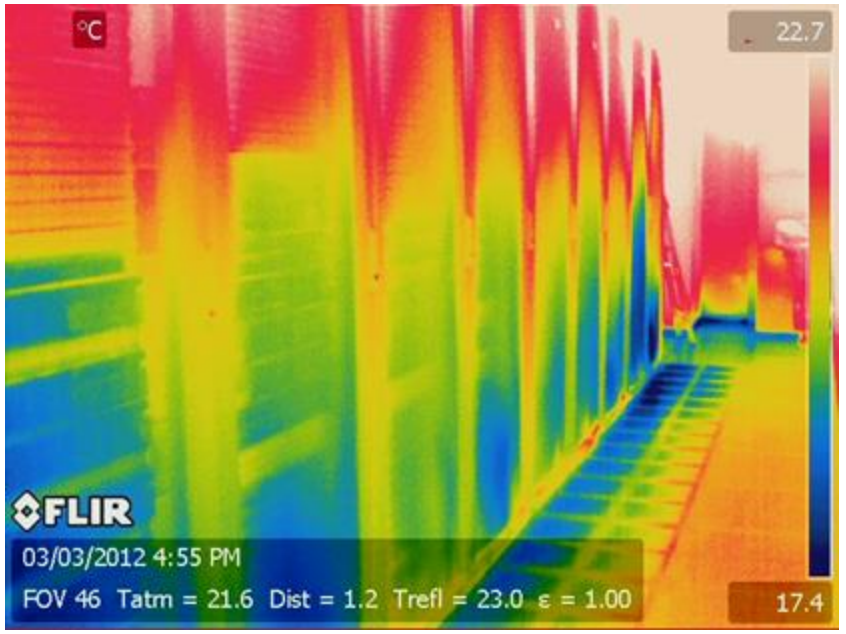
TRNG Output


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

More on PUF Applications

Motivation: Securely Sensing without Key

- Physical features should be closely monitored
  - The temperature of data center, Facebook, Google, Amazon, etc



Motivation: Securely Sensing without Key

- Physical features should be closely monitored
  - The temperature of data center, Facebook, Google, Amazon, etc

- Some physical features might be meaningful for security/privacy
  - Relative location between bank cards and automated teller machines (ATMs), card (not) present withdrawal

Motivation: Securely Sensing without Key

- Physical features should be closely monitored
  - The temperature of data center, Facebook, Google, Amazon, etc

- Some physical features might be meaningful for security/privacy
  - Relative location between bank cards and automated teller machines (ATMs), card (not) present withdrawal

Motivation: Securely Sensing without Key

- Physical features should be closely monitored
  - The temperature of data center, Facebook, Google, Amazon, etc
- Some physical features might be meaningful for security/privacy
  - Relative location between bank cards and automated teller machines (ATMs), card (not) present withdrawal
- Some physical features are hard to sense but favoring many applications
  - Digital rights management, physically/irreversibly canceling membership?

- Secure sensors are needed:
  - Operation safety, secrecy of sensitive data

Key Is a Target

- Modern security protocols are commonly based on secret keys.
- A robust key enhances the robustness of security systems, but also announces itself as an interested target for attackers. [1]

[1] Rivest, Ronald L. Illegitimi non carborundum. CRYPTO (2011).