Survey of Hardware Random Number Generators (RNGs)

Dr. Robert W. Baldwin
Plus Five Consulting, Inc.
Outline

• True vs. Pseudo Randomness
• Radiation Noise RNG
• Removing Bit-Bias
• Thermal Resistive Noise RNG
• Diode Breakdown Noise RNG
• Summary
Importance of Randomness

• Generate Long-Term Cryptographic Keys
  – Ensure That Breaking One Key
    Does NOT Help Break Other Keys

• Generate Challenges That Have Never Been Used Before
  – Input To US Gov. Digital Signature Algorithm
What is True Randomness?

- Accepted Examples
- Unacceptable Examples
- Criteria
Accepted Examples

• Toss Coin & Call-It In The Air
  – This Has Two RNGs: Coin & Caller
  – Tries To Avoid Flipper’s Influence

• Lots of Experience Confirms
  – Outcome Hard To Control
  – Short Toss Is Not Acceptable
  – Initial Conditions Don’t Matter
Accepted Examples

• Wheel of Fortune or Roulette Wheel
  – Short Spin Is Not Acceptable
• Simple Tamper Detection
  – Can Verify Lack of Control
• Better Randomness
  Takes Longer
Unacceptable Examples

- Card Shuffling By Expert
- Lots of Experience With This
  - Some People Can “Break” It
- Design Allows For Undetected Manipulation
Unacceptable Examples

- $X = \text{Encrypt}(\text{Key1}, N) \oplus \text{Encrypt}(\text{Key2}, N)$
  $N = N + 1$
  - Keys Chosen By Government But In Hardware
- $X$ Values Pass All Statistical Tests If Encrypt Function Is Strong
  - Like AES Candidates With Large Key and Block Sizes
- Must Trust Key-Holders
- If Keys Revealed, Easy To Find All Past And Future Output Values
Criteria For Randomness

• All Statistical Tests Should Not Distinguish Generated Values From Theoretical Sequence of Independent Uniformly Distributed (IUD) Bits.
  – “Uniform” Means 50-50 chance of One or Zero
  – “Independent” Means Bits Not Related
  – “All Tests” Means The Ones We Have Thought Of So Far
Criteria For True Randomness

• Output Hard To Influence
  – Temperature, Vibration, RF, Power, Etc.

• Knowledge Of Past Outputs Does Not Help Predict Future Outputs
  – Even If Attacker Has Lots Of Information and Computational Resources
Is True Randomness Possible?

• Newton: No
  – Position & Velocity $\rightarrow$ Future

• Heisenberg: Yes
  – Cannot Know Both At Same Time

• Schoedinger: Yes
  – Probability Waves Are Fundamental

• Gibbs, Helmholtz: Yes
  – Entropy Implies Information Is Lost
Outline

• True vs. Pseudo Randomness

 Radiation Noise RNG
  • Removing Bit-Bias
  • Thermal Resistive Noise RNG
  • Diode Breakdown Noise RNG

• Summary
Radiation Noise RNG

• General Idea:
  Radioactive Material Produces Decay Particles at Unpredictable Intervals.

• Construction

• Theory

• Engineering Issues

• Randomness Properties
Construction of Radiation RNG

• Detect Decay and Convert to Binary

- Radioactive Source
- Detector
- Whitening (remove bias)
- Digitizer
- Clock
Theory of Radiation RNG

- Krypton Decay to Rubidium

\[ \text{Kr}^{85} \rightarrow \text{Rb}^{85} + e^- + \gamma \]
Theory of Radiation RNG

- Atoms Decay Independently
- Decay Follows Poisson Distributions
- Event Count
  - Time Interval
  - Radioactivity
Engineering Issues

• Can Use Low-Level Background Radiation for Low Bit-Rates
• High Bit-Rates Require High Radiation
• Radiation Harms Other Components
• Extensive Safety Regulations and Laws
Engineering Issues

- Vacuum Tube Detectors Are Large and Require High Voltage
- Silicon Detectors Fatigue With Usage
- Hard To Shield Against Attacker Influencing Radiation Level
Randomness Properties

• Independent, But Non-Uniform Bits
  – Chance of Detection Increases With Time Window. Hard to Get Exactly 50-50
  – Decay Rate Decreases Over Years

• Problem: How Remove Bias in Bits?
Outline

• True vs. Pseudo Randomness
• Radiation Noise RNG

Removing Bit-Bias
• Thermal Resistive Noise RNG
• Diode Breakdown Noise RNG
• Summary
Whitening Algorithms

- Purpose Is To Remove Bias
- “White Noise” – From Audio Engineering Like Hiss on a Radio
- Means Equal Energy in All Frequency Bands
  - Analog Equivalent of IUD Bits
VN Whitening Algorithm

- Von Neumann Algorithm

1. Sample Two Equal Sized Time Intervals.
2. If Neither Detects Decay, go to 1.
3. If Both Detect Decay, go to 1.
4. Output Zero if First Detected Decay, Else Output One.
VN Whitening Algorithm

- Let $p =$ Probability of Decay in Interval
- Let $q = 1 - p =$ Probability of No Decay
- Probability of Outputting Zero:
  $$(p \times q) / ((p \times q) + (q \times p)) = \frac{1}{2}$$

<table>
<thead>
<tr>
<th></th>
<th>No Clicks</th>
<th>1st Click</th>
<th>2nd Click</th>
<th>Both Clicks</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q \times q$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p \times q$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$q \times p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$p \times p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VN Whitening Algorithm

• Advantage
  – Provably Removes Bit-Bias

• Drawbacks
  – May Have To Wait A Long Time to Generate Next Bit
  – Bias in Size of Time Intervals Used To Sample Events Will Show Up in Output
Hash Whitening Algorithm

• Gather N Bits, Reduce to M Bits
• Ex: 8 → 1 Output Parity of Raw Byte
• Ex: M-Bit Linear Feedback Shift Register
  – Each Output Value Produced by $2^{(N-M)}$ Inputs
  – Hope Hash Mapping Is Unrelated to Bit Bias
• Runs in Fixed Time
• Slower Process Produces Better Bits
Outline

• True vs. Pseudo Randomness
• Radiation Noise RNG
• Removing Bit-Bias
• Thermal Resistive Noise RNG
• Diode Breakdown Noise RNG
• Summary
Thermal Resistive Noise RNG

• General Idea:
  Voltage Across Resistor Varies Randomly Due To Vibration of Atoms.

• Construction

• Theory

• Engineering Issues

• Randomness Properties
Construction of Thermal RNG

- Amplify Variation and Digitize It

Diagram:

- Power
- Metal Film Resistor
- Fixed Current Sink
- Amplifier
- Digitizer
- Clock
Theory of Thermal RNG

• Electrons Loose Energy as They Pass Through Atoms of the Resistor.
  – Electrons Collide With Atoms
  – Rebound in Unpredictable Directions
• Lost Energy Heats-Up the Resistor
  – Light Bulb Filaments Get Hot Enough to Glow
• Voltage Across Resistor = Total Loss
Theory of Thermal RNG

- Collision Governed by Quantum Mechanics
- Rebound Depends on Atom’s Vibration
Theory of Thermal RNG

• Johnson: Thermal Noise Has Equal Energy In All Frequency Bands

• $P(\Delta f) = 4 k T R \Delta f$
  Power of Noise Signal is Proportional to Boltzmann Constant, Temperature, Resistance, and Bandwidth
Theory of Thermal RNG

Johnson Noise
Metal Film Resistors

Fit Results
$e_n = 6.4 \text{nV}$
$C = 22 \text{ pF}$

$e_n^2 [\text{V/Hz}^2]$ vs $f [\text{Hz}]$
Engineering Issues

• Ordinary Resistors: Additional Noise
  – Tube Packed With Carbon Particles
  – Humidity, Vibration, RF, Static Electricity

• Metal Film Resistors: Just Thermal Noise
  – Easy To Fabricate on Silicon
  – RNG Operates at Low Chip Voltages
Engineering Issues

• Easy to Shield From Influence
  – Attacker and Other Components in System
• Must Filter Power Supply To Amplifier
• Digitizer and Amplifier Limit Bit-Rate
• Whitening Still Helpful
Randomness Properties

- Raw Bits Have Excellent IUD Statistics
  - Within Bandwidth of the Device
- Noise Energy Varies With Temperature
  - But Remains Uniform
- Collisions Depends on Quantum Scattering
- Rebound Depends on Vibration of Each Atom (Temperature)
Outline

• True vs. Pseudo Randomness
• Radiation Noise RNG
• Removing Bit-Bias
• Thermal Resistive Noise RNG
• Diode Breakdown Noise RNG
• Summary
Diode Breakdown Noise RNG

• General Idea:
  Reverse Current Through Diode Varies Randomly Due To Tunneling of Electrons.

• Construction

• Theory

• Engineering Issues

• Randomness Properties
Construction of Diode RNG

• Amplify Current Variation and Digitize It

Diagram:
- Power
- Reversed Diode
- Current To Voltage Amp
- Digitizer
- Clock
- Ground
Theory of Diode RNG

• P-N Junction Acts as One-Way Gate
• Electrons Easily Flow From P to N Regions
  – Only Loose 0.6 Volts of Energy
• Reverse Flow Requires 10 to 30 Time More
  – 6 to 18 Volts

Ground ———P-Region|P-N|N-Region——— Power
Theory of Diode RNG

• Rate of Reverse Flow Depends On:
  – Thermal Resistive Effects
  – Avalanche Breakdown Effect (Shot Noise)

• Thermal Effect Happens When Electron Crosses Junction In One Step
  – Dominant Effect for Larger Reverse Voltage
Theory of Diode RNG

• Avalanche Begins When Electrons Pile-Up Part-Way Across P-N Junction
• First Electron Stuck in Middle Makes It Easier for Next Electron To Get That Far
• When Enough Electrons Build Up They All Jump Across Remaining Distance
• Observed as Pulse or Shot of Current
Theory of Diode RNG

• Avalanche (Shot) Noise is Not Uniform
• High Frequency Noise Less Likely Due to Time Needed to Reload the Avalanche
• $P(\Delta f) = \frac{2qI\Delta f}{f}$
  
  Power of Noise Signal is Proportional to Electron Charge, Current, Bandwidth and Inversely Proportional to Frequency
Theory of Diode RNG

Shot and Thermal Noise

\[ \frac{e_r}{\sqrt{\text{Hz}}} \]

\[ f \text{ [Hz]} \]

- Blue: Thermal
- Green: Shot
Engineering Issues

• Diodes Easy to Fabricate on Chips
• Reverse Voltage Higher Than CPU Uses
• Voltage Must Be Controlled to Balance Avalanche vs. Thermal Noise
• Post-Processing Required to Remove Bias Favoring Lower Frequencies
Randomness Properties

- Output Combines Avalanche & Thermal
  - Biased Towards Low Frequencies
- Unpredictable Due To Quantum and Chaotic Avalanche Effect
- Noise Energy Spectrum Changes With Temperature and Voltage
Outline

• True vs. Pseudo Randomness
• Radiation Noise RNG
• Removing Bit-Bias
• Thermal Resistive Noise RNG
• Diode Breakdown Noise RNG

⇒ Summary
Summary

• Practical Designs Can Produce “True” Random Numbers
  – Past Output Cannot Predict Future
  – Hard For Attacker To Influence

• Well Understood Theory & Engineering

• Thermal Resistive Well Suited to VLSI

• High Bit-Rates Conflict With High Quality