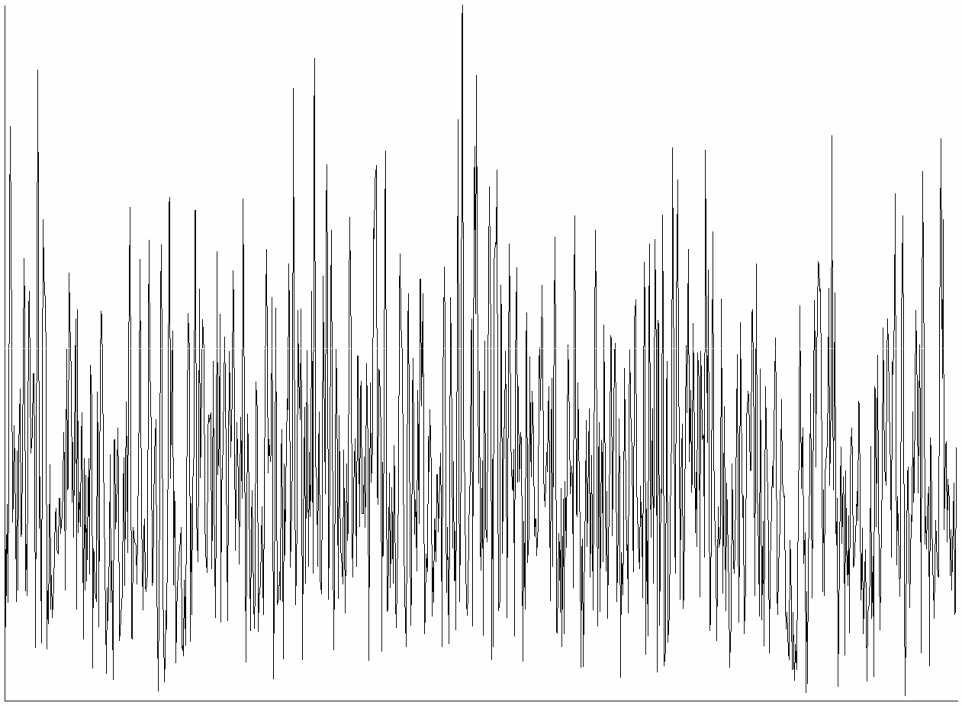
4.1 Weißes Gaußsches Rauschen

Eine Möglichkeit, echte Zufallszahlen zu erzeugen, besteht darin, weißes Gaußsches Rauschen auszuwerten. Bei weißem Rauschen handelt es sich um eine Hintergrundfrequenz in elektromagnetischen Systemen die unabhängig von der Frequenz das gleiche Leistungsspektrum hat (Analogie zu weißem Licht). Schrotrauschen entsteht, da bei einem makroskopisch fließenden Strom die einzelnen Stromimpulse der Elektronen nicht unbedingt gleichmäßig, sondern zu voneinander unabhängigen Zeiten auftreten. Der Gesamtstromfluß setzt sich aus den Beiträgen der einzelnen Ladungsquanten (Elektronen) zusammen, wobei ein einzelnes Elektron zu einem Stromfluss führt. Dieser hängt vom Aufbau des zu betrachtenden Bauteils ab.



Zur Erzeugung von Zufallszahlen greift man zu unterschiedlichen Zeiten Messwerte ab und vergleicht diese folgenderweise miteinander:
Ist:
$u(ti) \geq u(ti+1)$ folgt daraus eine 0 als Ausgabe

u(ti) < u(ti+1) folgt daraus eine 1 als Ausgabe
Durch das Durchführen längerer Messstrecken könnte man so schnell große Zahlen zufällig generieren. Da das komplette System auf physikalisch nicht deterministisch nachvollziehbaren, also für unser momentanes Verständnis vollkommen zufälligen Effekten beruht, handelt es sich hier um echte nicht vorhersehbare/rekonstruierbare Zufallszahlen.
Die technische Umsetzung dieser Zufallszahlengeneratoren ist meist eine PCI-Karte. Sie besteht im wesentlichen aus einer Rauschquelle (Diode/Wiederstand/Glühkathode) einer Abtastschaltung und einem Taktgenerator. Wegen leichter Beeinflussung von solchen elektrischen Systemen durch elektromagnetische Felder sind diese Karten in geschlossene hochfrequenz-dichten Eisengehäusen verbaut.

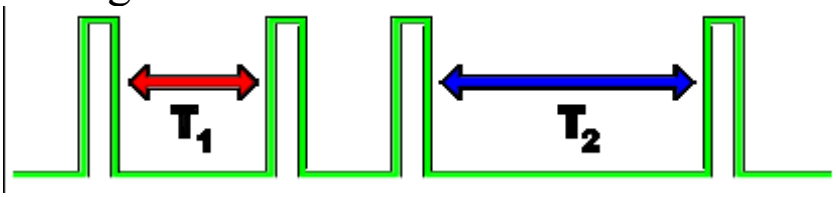
4.2 Radioaktiver Zerfall

Beim Bestimmen von Zufallszahlen mit Hilfe des radioaktivem Zerfalls bedient man sich der Tatsache, dass man zu jedem Isotop nur die Halbwertszeit beziffern, allerdings nicht den genauen Zeitpunkt des Zerfalls eines einzelnen Atoms vorhersehen, kann. In den Zufallszahlengeneratoren, die den radiaktiven Zerfall auswerten, wird meistens Caesium 137 benutzt, welches auch bei Atomuhren oder in der Krebstherapie Verwendung findet. Caesium 137 hat eine Halbwertszeit von 30,17 Jahren. Ablauf des Zerfalls: Damit ein Atom sich in ein anderes verwandeln kann, muss eines der atomaren Teilchen aus dem Atomkern die Potentialbarriere überschreiten. Dies ist nach der Vorstellung der klassischen Physik nicht möglich da die Energie zur Überwindung des Coulombwalls hinzugeführt werden muss, was nur durch den Tunneleffekt erklärbar ist. Der Tunneleffekt ist ein

quantenmechanischer Effekt der den Teilchen das Unterwandern dieser Potentialbarriere ermöglicht.
Nach dem Unterwandern der Potentialbarriere gibt das Caesium ein Elektron (β −) sowie ein Elektron-Antineutrino ab, und wird dadurch zu Barium 137m in einem angeregten Zustand. In der Halbwertszeit von 156 Sekunden begibt dieses sich in den stabilen, nicht radioaktiven Zustand, Barium137, unter Abgabe eines γ - Quantums.

$$^{137}\mathrm{Cs} \xrightarrow{30.17\mathrm{y}} {}^{137\mathrm{m}}\mathrm{Ba} + \beta^- + \overline{\nu_e} \xrightarrow{156\mathrm{s}} {}^{137}\mathrm{Ba} + \gamma$$

Mit Hilfe eines Geiger-Müller-Zählrohres misst man das Auftreten der Strahlungen und überträgt diese an den Rechner. Durch das Erzeugen von Zeitintervallen zwischen den einzelnen Zerfällen und den Vergleich dieser miteinander kann man so Zufallsbits erzeugen.



Wenn T1 > T2 erzeugt der Generator eine 1, andern falls eine 0. Sollten die Intervalle gleich lang sein, werden sie verworfen und neue Werte gewählt.
Alternativ ist es auch möglich, die Anzahl der Zerfälle innerhalb eines festgelegten Intervalls zu messen, diese mit einer Ganzzahldivison durch 2 zu verarbeiten und den Rest dieser Berechnung als Zufallsbit zusetzen. Der Vorteil dieses Verfahrens ist die Güte der Zufallszahlen, da die quantenmechanischen Vorgänge beim Zerfall von Atomen nicht deterministisch erklärbar sind und die Ausgabe relativ schnell erfolgen kann.
Ein erheblicher Nachteil ist allerdings, dass man, um dieses Verfahren zu nutzen, einen radioaktiven Stoff in der Nähe seines Rechners platzieren muss, was unter gesundheitlichen Aspekten bedenklich werden könnte.