Kuriose Nachrichten

Beitrag von „Volker_D“ vom 6. September 2025 09:50

> Zitat von SteffdA
>
> Das kann man schon lange. Dafür reicht eine Diode oder ein Widerstand und ein A/D-Wandler.
>
> Aber ich dachte beisher immer, dass es wegen der Entschlüsselung reproduzierbare Zufallszahlen (Pseudozufallszahlen) für die Kryptografie braucht.

Ja, vorallem für Primfaktorzerlegung.

Aber das mit Diode, Widerstand und A/D Wandler ist gar nicht so leicht wie du denkst. Auch das ergibt keine "guten" Zufallszahlen.

Warum? Weil es von deiner Umgebung abhängt. Kannst du leicht an Arduino, Raspberry Pi und Co prüfen. Da kannst du auch auch einfach den analogen EIngang zum lesen benutzen um Zufallszahlen zu erzeugen. Hat aber 2 große Nachteile:

a) Diese Zufallszahlen können nur relativ langsam abgefragt werden. Wenn du also viele Zufallszahlen brauchst, dann ist das nicht zu gebrauchen.

b) Diese Zufallszahlen sind statistsich leider gar nicht so zufällig, wie gute Zufallszahlen sein müssen. Klar, wenn du es nur ein einziges mal machst/gebrauchst, dann ist es zufällig genug. Brauchst du aber viele Zufallszahlen und oder große Zufallszahlen (und setzt diese also aus vielen Zufallszahlen zusammen. Beim Arduino hast du ja z.B. nur einen 10 bit AD Wandler, kannst also gerade mal eine "zufällige" Zahl zwischen 0 und 1023 machen, dann brauchst du viel mehr AD Wandler. Und die Zahlen sind untereinander nicht zwingend unabhängig. Ist eigentlich egal wie du es machst, ob mit fotowiderstand, Kamera, ... Ja, dass sind Hardware zufallszahlen, einmalig ok. Für viele Zufallszahlen aber leider viel zu unzufällig und vorhersehrbar bzw. stark eingrenzbar.