物理乱数で電子サイコロをつくる

物理現象によって作られる乱数を物理乱数といいます。 直方体のサイコロを振ると1から6までの物理乱数が得られます。 物理乱数は原理的に予測できないため、公平に物事を選んだり、 パスワードなど他人に知られにくい情報を得るのに使えます。 今回の展示では、トランジスタを逆接続して、なだれ降伏と いう現象を起こすことで予測できない雑音を生成しています。 その雑音をArduino UNOで処理することで、1から6までの数が 同じ確率で出てくる電子サイコロを作ることができました。 この電子サイコロと同じ技術は、情報セキュリティ技術の 現場でも活用されています。

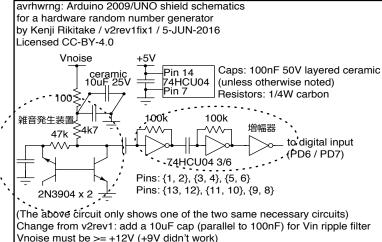
Arduino UNO R3 avrhwrng 1/2 ATmega328P LED表示装置 MCUを使って 雑音 フォンノイマンフィルタ 増幅器 発生装置 を使って3ビットの 物理乱数を得る 得た値は0から7まで 液晶表示装置 なので avrhwrng 2/2 (2行で表示) 0と7を捨てて 1から6までの値を得て 1秒に1回ずつ 液晶 (LCD) シリアルポート 雑音 **USB** 増幅器 **LED** 経中でパソコン 発生装置 につなげられる シリアルポート Vnoise can be supplied from Arduino Vin or a DC-DC converter (9600bps) の3つに出力する

Maker Faire Tokyo 2016 理科教育研究フォーラム 展示作品 設計・制作: 力武 健次 (りきたけ けんじ、力武健次技術十事務所 所長) GitHub: @jj1bdx http://rikitake.jp/ (Document Version 1.0)

この装置では物理乱数の品質を高めるために、フォンノイマンフィルタという 方法を使っています。1ビットの乱数を得るために、あえて2ビット取得した上で 連続する同じビットを使わないことで、結果の確率を1/2にすることができます。

1つ日 2つ日 同じビットが連続しているので捨てて再度2ビット取得する 違うビット同士なので1つ目の「0」を結果として使う 違うビット同士なので1つ目の「1」を結果として使う 同じビットが連続しているので捨てて再度2ビット取得する

> →雑音発生装置と増幅器の回路図 詳しくは https://github.com/jj1bdx/avrhwrng/



↓さらに詳しい情報は以下のURLを見てね! https://github.com/jj1bdx/avrdice/