Hardvérový generátor náhody

Su dve druhy generátorov náhodných čísel: pseudonáhodné a pravé. Tie pseudonáhodné su tvorené algoritmom. Teda pokiaľ poznám algoritmus a jeho počiatočný stav, teoreticky som schopný vypočítať každé číslo, ktoré takýto algoritmus "náhodne" vygeneruje. Pravý generátor náhodných čísel generuje čísla, ktoré nie je možné predovedať. Takéto pravé generátory zvačša používajú nejaký fyzikálny fenomém ako zdroj náhody.

Tento obvod používa na generovanie náhodného signálu lavínový šum vznikajúci pri prieraze diódy. Tento šum je ďalej zosilený a spracovaný na digitálny signál. Takto obvod môže slúžiť ako zdroj náhody. Na digitalizovanie signálu na výstupe sme použili programovateľný modul Arduino.

Obvod

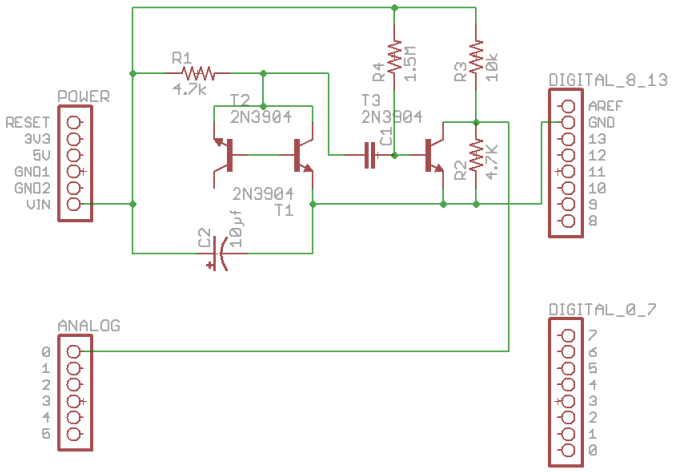

Figure 1: Schéma obvodu.

Obvod je napájaný z $12V$ externého zdroja cez vstup Vin a signál je privedený na A-D prevodník $A0$ na doske Arduin-a. Tranzistory T1 a T2 majú spojené bázy a spolu umožnia generovanie lavínového šumu v záverne polarizovanom PN prechode. Tento šum je potom ďalej zosílený tranzistorom T3 a privedený cez rozdeľovač napätia na A-D prevodník A0.

Spracovanie nahodného signálu

Nahodný signál z prevodníka A0 je spracovaný programom bežiacim na Arduine a to nasledovne:

1. **Kalibrácia:** prvých 10 sekúnd je signál nahrávaný a určí sa jeho stredná hodnota.
2. **Vzorkovanie:** po každom ďalšom odčítaní údaju sa tento udáj porovná so strednou hodnotou. Ak je vačší ako stredná hodnota, výstup je 1. Inak je výstup 0.

Takto nám poskytuje tento obvod sekvenciu náhodne za sebou idúcich núl a jednotiek.

Tento výstup je ešte možné v rámci programu filtrovať napríklad von Neumannovým filtrom. Takýto filter zoberie zo vstupu dve posledné čísla. Pokiaľ sú obe rovnaké, napr. 11 alebo 00 tak ich zahodí. V prípade poradia 01 je výstup 1 a v prípade poradia 10 je výstup 0.

Hotové zariadenie

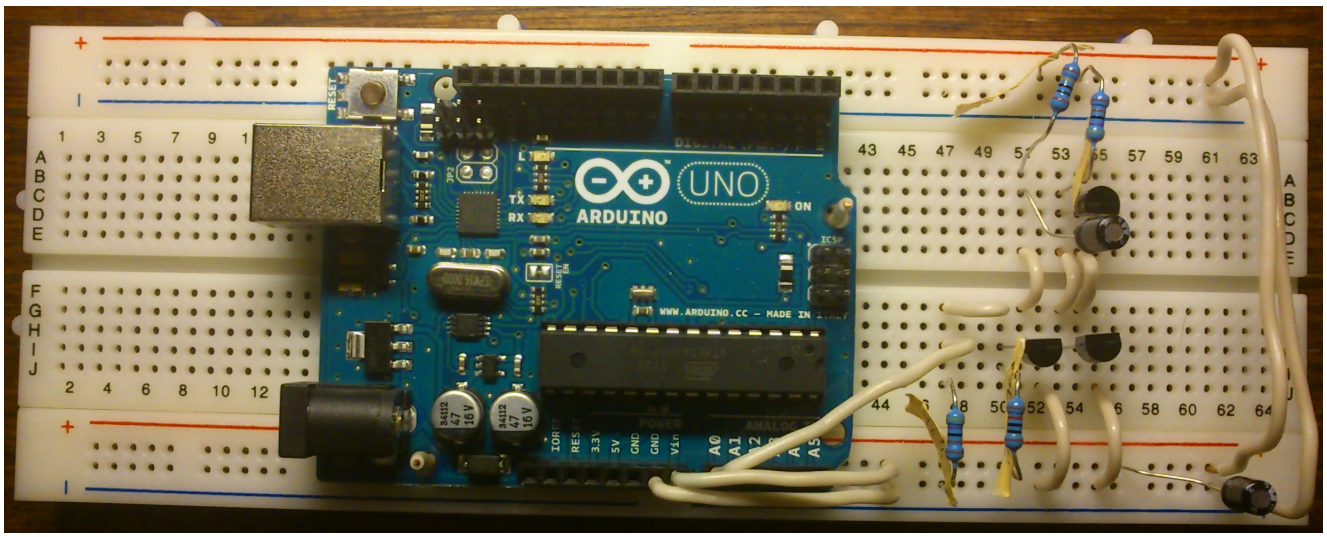

Figure 2: Fotografia už hotového zariadenia.

Zoznam súčiastok

Súčiastka	Počet	Súčiastka	Počet
Arduino	1	1, 5M Rezistor	1
2N3904 Tranzistor	3	0, 1μF Kondezátor	1
4, 7k Rezistor	2	10 μF Kondenzátor	1
10k Rezistor	1	12V DC Adaptér	1

Table 1: Menný zoznam súčiastiek.

Referencie

http://robseward.com/misc/RNG2/

http://cs.wikipedia.org/wiki/%C5%A0umov%C3%BD_gener%C3%A1tor