Kryptograficzna generacja liczb losowych wykorzystując szum śrutowy

Jakub Niemczuk[1], Ewa Popko[2], Sławomir Drobczyński[3], Tadeusz Martynkien[3]

1. Wydział Elektroniki Mikrosystemów i Fotoniki, Politechnika Wrocławska, ul. Janiszewskiego 11/17, 50-372 Wrocław
2. Katedra Technologii Kwantowych, Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska, Wyb. Wyspiańskiego 27, 50-370 Wrocław
3. Katedra Optyki i Fotoniki, Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska, Wyb. Wyspiańskiego 27, 50-370 Wrocław

WSTĘP

Wraz z rozwojem telekomunikacji zwiększyło się zapotrzebowanie na nowe skuteczniejsze mechanizmy szyfrowania kanałów komunikacyjnych. Wiele algorytmów wykorzystuje liczby losowe do inicjalizacji szyfrowania lub generacji kluczy, a ich moc zależy od jakości wykorzystywanych generatorów liczb losowych. Aktualnie stosowane generatory oferujące najwyższą entropię wykorzystują zjawiska kwantowe, takie jak: fluktuację próżni, elektroluminescencja, rozpad radioaktywny, zjawisko Ramana. Prezentowany sposób generowania liczb losowych oparto na szumie śrutowym generowanym w półprzewodnikach. Celem projektu było wykonanie odpornego na zakłócenia i czynniki zewnętrzne generatora liczb losowych, opartego na zjawisku elektroluminescencji i szumu śrutowego generowanego w fotodiodzie działającej w konfiguracji fotodetektora.

SZUM W PÓŁPRZEWODNIKACH

Wszystkie elementy półprzewodnikowe podczas pracy są źródłem szumu elektronicznego. Na szum wytwarzany przez zwykłe złącze PN składają się: [1]
- Szum termiczny,
- Szum śrutowy,
- Szum generacji – rekombinacji,
- Szumy $1/f^{\alpha}$,
- Szum przebicia lawinowego.

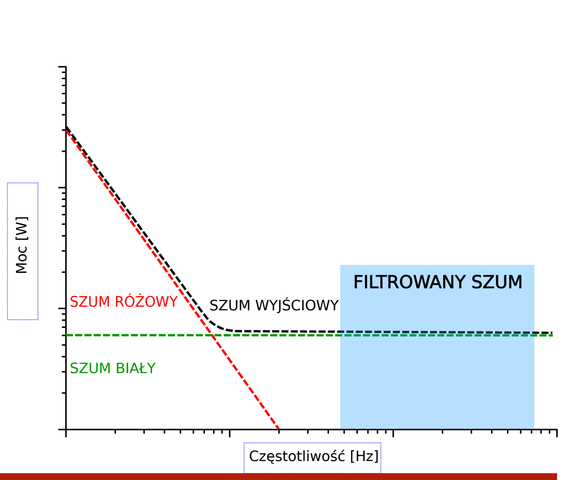
Powyższe składowe odgrywają większa bądź mniejszą rolę w zależności od budowy złącza jak i parametrów pracy (napięcie, prąd, temperatura, czynniki mechaniczne, promieniowanie jonizujące).

Szum śrutowy wywodzi się z nieciągłości prądu elektrycznego. Ładunek elektryczny w postaci elektronów pokonuje bariery potencjału w różnym czasie. Wartość skuteczną zmian prądu opisuje poniższe równanie.

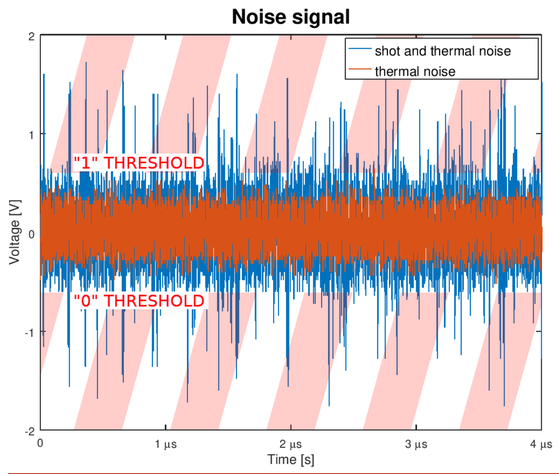
$$i_n = \sqrt{2qI\Delta f}$$

Gdzie:
q – Wartość ładunku elementarnego,
I – Natężenie prądu,
Δf – Pasmo mierzonego szumu.

KWANTYZACJA SZUMU

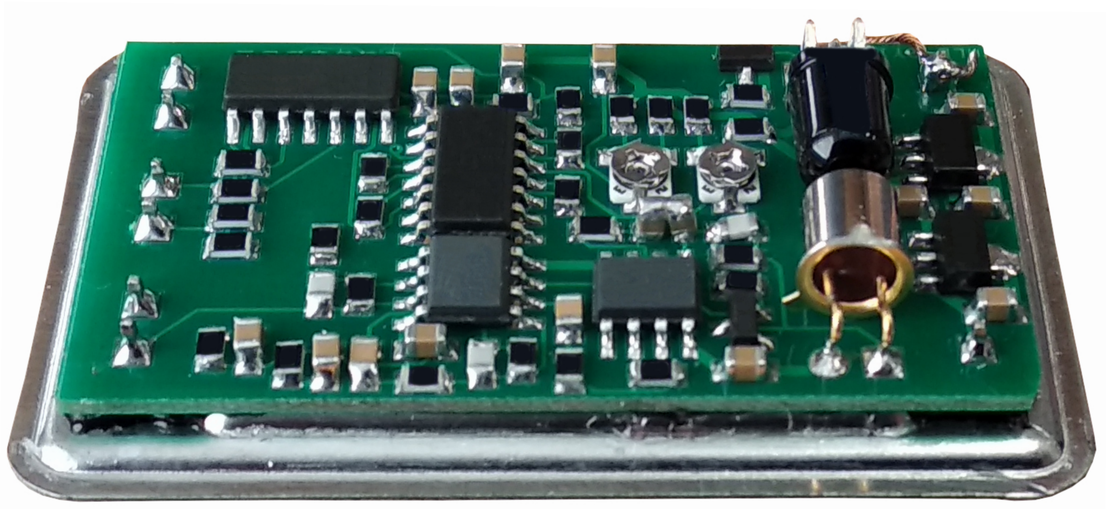


Rys. 1 Wykres mocy szumu generowanego przez element półprzewodnikowy z podziałem na szum różowy (1/fα) i biały (termiczny i śrutowy)

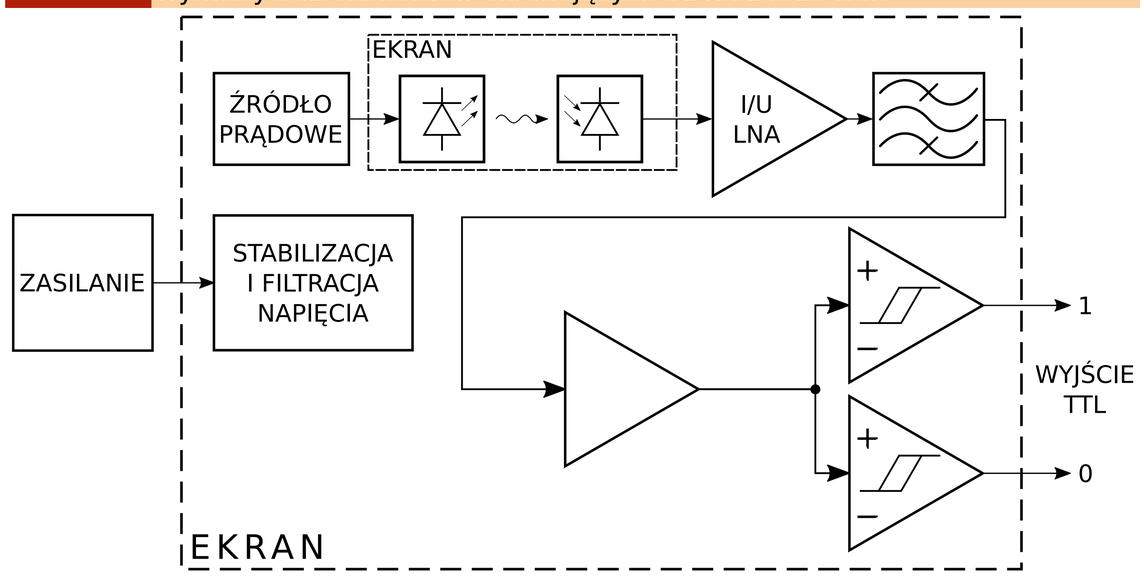


Rys. 2 Oscylogram przedstawiający amplitudy szumu termicznego układu i szumu całkowitego po oświetleniu fotodiody

REALIZACJA URZĄDZENIA



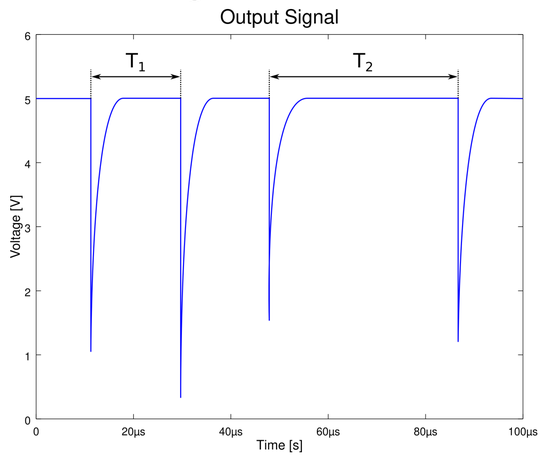
Rys. 3 Zdjęcie przedstawiające skonstruowane urządzenie
Wymiary bez elementów ekranujących 51 x 32 x 10 mm



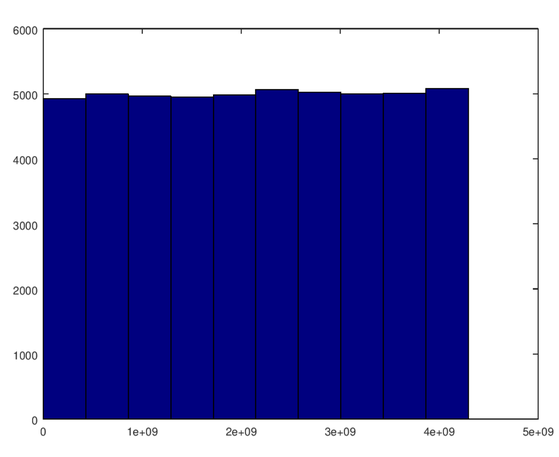
Rys. 4 Schemat blokowy urządzenia

WYNIKI

Histogram sekwencji danych pozyskanych metodą porównywania czasów pomiędzy parami impulsów ma płaski rozkład oraz pomyślnie przechodzi wszystkie testy z pakietu NIST [2] z wyjątkiem testu uniwersalnego.



Rys. 5 Oscylogram przedstawiający ideę generacji bitów metodą porównywania czasów pomiędzy parami impulsów



Rys. 6 Histogram 50000 liczb typu uint32 wygenerowanych metodą porównywania czasów pomiędzy parami impulsów

[1] Alicja Konczakowska, B. M. Wilamowski. *Noise in Semiconductor Devices - Industrial Electronics Handbook*, vol. 1 Fundamentals of Industrial Electronics, 2nd Edition, chapter 11, pp. 11-1 to 11-12, CRC Press 2011.

[2] *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*, NIST SP 800-22rev1a, National Institute of Standards and Technology.

supported by project NCBiR POIR.01.01.01-00-0173/15