Fundusze Europejskie Inteligentny Rozwój

Projekt realizowany w ramach Programu Operacyjnego Inteligentny Rozwój, poddziałanie 1.1.1 "Badania przemysłowe i prace rozwojowe realizowane przez przedsiębiorstwa", współfinansowany ze środków Budżetu Państwa oraz Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Ekspertyza uzupełniająca w zakresie badań w ujęciu teorii mechaniki i informatyki kwantowej nad właściwościami ciągów liczb prawdziwie losowych generowanych w toku zjawisk kwantowych oraz teoretyczno-eksperymentalnych badań w dziedzinie mechaniki i informatyki kwantowej w zakresie wybranych procesów kwantowych mogących być wykorzystanymi do generacji liczb prawdziwie losowych

W. A. Jacak, J. E. Jacak, W. A. Donderowicz, L. Jacak

Wstęp

W ostatnich latach obserwuje się niezwykły wzrost zainteresowania generatorami liczb losowych. Zbiór liczb losowych jest niezbędny w wielu dziedzinach współczesnej nauki i technologii a także w życiu codziennym. Jest konieczny do symulacji zjawisk fizycznych. Stanowi podwaliny kryptografii, która zapewnia bezpieczeństwo komunikacji cyfrowej. Wreszcie na liczbach losowych opierają się systemy gier (loterie i automaty do gier). Do niedawna generacja liczb losowych polegała na wykorzystaniu oprogramowania komputerowego: zadany wyjściowy zestaw liczb służył do generacji ciągu liczb losowych według zadanego algorytmu. Taki generator, zwany pseudo-generatorem liczb losowych (ang. Pseudo-Random Number Generator, PRNG) w rzeczywistości generuje ciągi, które nie są losowe i w związku z tym jest narażony na możliwość odszyfrowania. Tymczasem istnieje bogata klasa fizycznych zjawisk kwantowych, które charakteryzuje nieprzewidywalność. Brak determinizmu w przypadku tych zjawisk spowodował dynamiczny rozwój badań aplikacyjnych mających na celu stworzenie generatora liczb losowych opartego o efekty kwantowe.

Generatory tej klasy rozwiązań nazywane są prawdziwymi albo kwantowymi generatorami liczb losowych (ang. True/Quantum Random Number Generator, TRNG/QRNG). Te ostatnie są już dostępne komercyjnie (ID Quantique, 2014; Micro Photon Devices, 2014; PicoQuant, 2014; QRB121, 2014; Quintessence Labs, 2014; Qutools, 2014; Wilber, 2014; Hughes and Nordholt, 2016). Dostępne są również serwery online, które zapewniają kwantowe liczby losowe na żądanie[1]. Z oczywistych względów bezpieczeństwa w szczególności w odniesieniu do kryptografii, pożądane jednak jest takie rozwiązanie, które będzie w pełni zaufane. Oprócz tego kluczowego warunku, QRNG powinien spełniać jeszcze szereg oczywistych wymagań m.in. cechować się jak największą szybkością generacji (liczba bitów/s), prostotą rozwiązania, niską ceną, małymi gabarytami, łatwością obsługi etc.

QRNG składa się z dwóch głównych elementów: źródła entropii oraz bloku przetwarzania (ang. post-processing). Źródłem entropii jest układ fizyczny, który generuje pewną losową wielkość fizyczną oraz układ pomiarowy, który ją wykrywa. Zwykle mierzona jest wielkość analogowa i aby wygenerować ciąg liczb losowych, sygnał analogowy musi

[1] M. Herrero-Collantes and Garcia-Escartin: Quantum random number generators, Reviews of Modern Physics, **89**, 015004-1-015004-48 (2017).

zostać przekształcony w sygnał cyfrowy. Taka operacja wymaga zastosowania konwertera analog-cyfra (AD). Zarówno sam pomiar jak i konwersja AD wprowadzają niepożądany determinizm. Rolą bloku przetwarzania jest ograniczenie łańcucha bitów do ciągu prawdziwych liczb losowych.

Pierwszy QRNG oparty był o zjawisko rozpadu promieniotwórczego. Wadą tego rozwiązania jest oczywista konieczność dysponowania źródłem promieniotwórczym, szybkość działania - generator oparty o to zjawisko jest wolny (kilkaset kbitów/s) i czas martwy detektora cząstek.

Najwięcej rozwiązań wykorzystuje optyczne zjawiska kwantowe. Należą do nich m.in. generatory w których źródłem entropii są pojedyncze nieskorelowane fotony, generatory z rozgałęzieniem ścieżki optycznej (np. w konfiguracji interferometru Macha-Zendera), oparte na statystyce czasu dotarcia impulsów, na zliczaniu pojedynczych fotonów, losowej fazie światła emitowanego przez laser, fluktuacjach fononów, próżni kwantowej i amplitudy szumu źródeł działających na zasadzie wzmocnionej emisji spontanicznej (ang. Amplified Stimulated Emission, ASE).

Z kolei klasa elektronicznych generatorów liczb losowych (ang. Electronic QRNG) oparta jest na kwantowych zjawiskach fizycznych występujących w przyrządach półprzewodnikowych, np. na efekcie tunelowym (m.in. efekt Zenera i efekt tunelowy w tranzystorze polowym MOS).

Oczywistym jest, że żadne z wymienionych rozwiązań nie gwarantuje perfekcyjnej losowości. Dlatego uzyskiwany na wyjściu generatora liczb losowych ciąg bitów jest poddawany testom statystycznym. Dwa główne zestawy testów, które służą do tego celu to test NIST (skrót ang. National Institute of Standards and Technology)[2] oraz DieHard[3] i ten ostatni – zmodyfikowany - DieHarder[4].

W niniejszym raporcie, przedstawiamy wyniki wstępnych propozycji realizacji QRNG. Spełnienie wszystkich ww. wymagań dotyczących QRNG jest bardzo trudne. Zdecydowaliśmy się wyjściowo na wyborze rozwiązania, które będzie gwarantować pełne zaufanie i cechować je będzie prosta architektura, niska cena oraz małe gabaryty. Z kolei modyfikacja mająca na celu zapewnienie dużej szybkości generacji planowana jest w dalszym horyzoncie czasowym.

I. Generator liczb losowych oparty na szumie śrutowym. Wersja I.

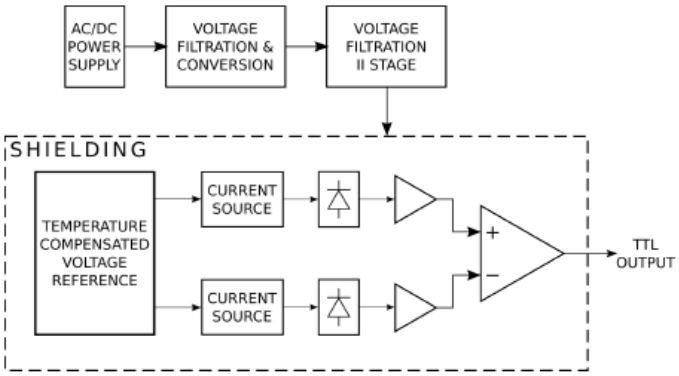
Pierwsza propozycja QRNG oparta jest o efekt Zenera w złączu p-n, spolaryzowanym w kierunku zaporowym. Rys. 1. przedstawia schemat blokowy generatora a rys. 2 zdjęcie generatora.

---

2 A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D. Banks, A. Heckert, J. Dray, S. Vo *et al.*, NIST special publication 800-22, 2010.

3 G. Marsaglia, Diehard: Aa battery of tests of randomness, http://stat.fsu.edu/geo/diehard.html, 1996.

4 http://www.phy.duke.edu/~rgb/General/dieharder.php



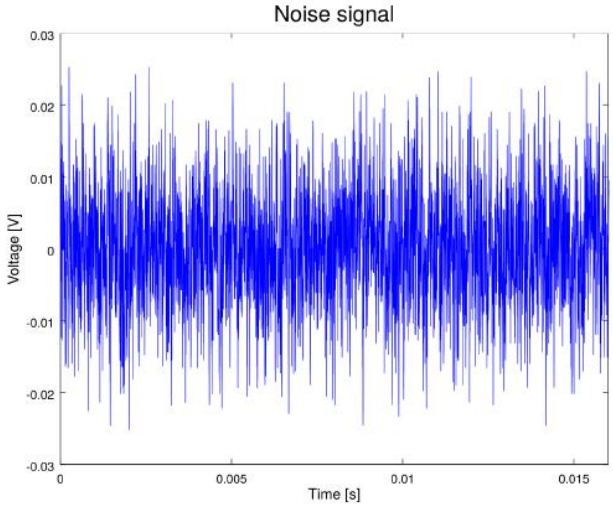
Rys. 1. Schemat blokowy generatora liczb losowych

Rys. 2. 74 x 53 x 10 mm

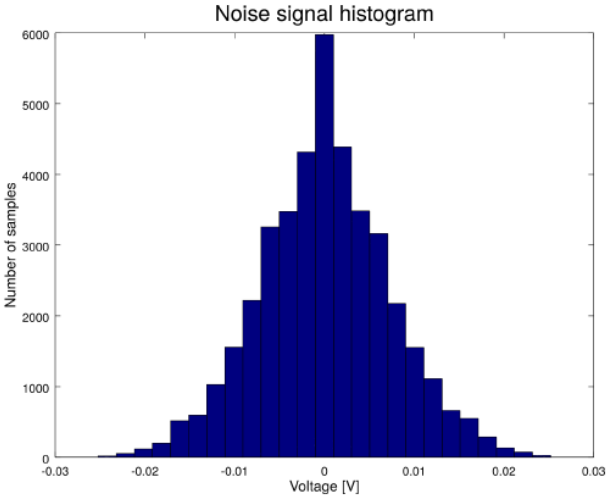
Projekt stanowi modyfikację rozwiązania zaproponowanego w pracy[5]. Generator składa się z dwóch głównych bloków. Pierwszy jest odpowiedzialny za konwersję napięcia i odfiltrowanie szumu pochodzącego od zasilania. Drugi blok, ekranowany przez stalową obudowę od wpływu zewnętrznego pola elektromagnetycznego, zawiera źródło dodatkowego napięcia odniesienia, które napędza dwa źródła prądu stałego pracujące w układzie zwierciadlanym.

Zastosowano dwa źródła prądowe aby wyeliminować dryft termiczny. Te źródła prądowe dostarczają prądu o natężeniu 10μA do złączy baza-emiter dwóch tranzystorów bipolarnych, spolaryzowanych w kierunku zaporowym napięciem równym 5V. Dwa sygnały szumu generowanego przez prąd wsteczny, przepływający przez złącza są wzmacniane, a następnie porównywane ze sobą przez komparator. Na wyjściu komparatora otrzymuje się ciąg bitów TTL. Rys. 3. Przedstawia wzmocniony sygnał z jednego ze źródeł szumu a rys. 4. rozkład statystyczny przykładowego sygnału szumów. Rozkład przypomina rozkład Poissona. Rys. 5. przedstawia przykładowy sygnał TTL.

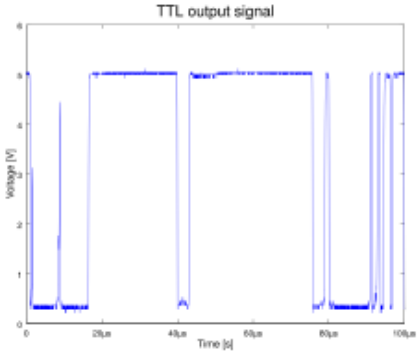
[5] Charles Platt, Aaron Logue. Really, Really Random Number Generator, Make: Projects, Make Magazine, 2016. https://makezine.com/projects/really-really-random-number-generator/



Rys. 3. Wzmocniony sygnał z jednego ze źródeł szumu. Próbkowanie co 400ns (RIGOL DS1054)



Rys. 4. Histogram przykładowego szumu (RIGOL DS1054).



Rys.5. Przykładowy sygnał TTL na wyjściu generatora.

Sygnał TTL został zebrany przy stałej częstości próbkowania za pośrednictwem mikrokontrolera AVR firmy Atmel i przesłany do komputera. Aby usunąć „bias”,

zastosowano metodę von Neumanna[6], która polega na pomijaniu w ciągu bitów tych, które się powtarzają.

Histogram losowo wybranego zestawu liczb po usunięciu „bias" w ilości 100000 przedstawia rys. 6. Rys. 7. przedstawia bitmapę (512 x 512 pikseli) losowo wybranych przykładowych danych. Nie obserwuje się żadnego powtarzającego się wzoru, co przemawia za losowym rozkładem. Losowość została poddana testom pakietu DieHarder[7].

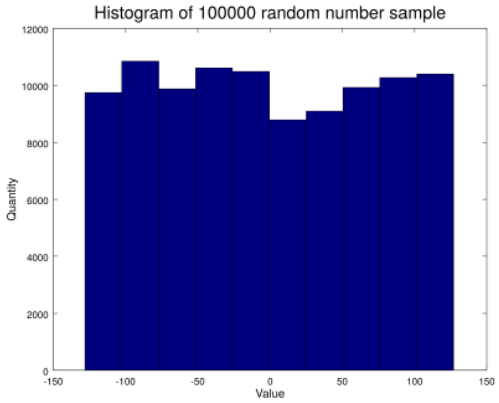
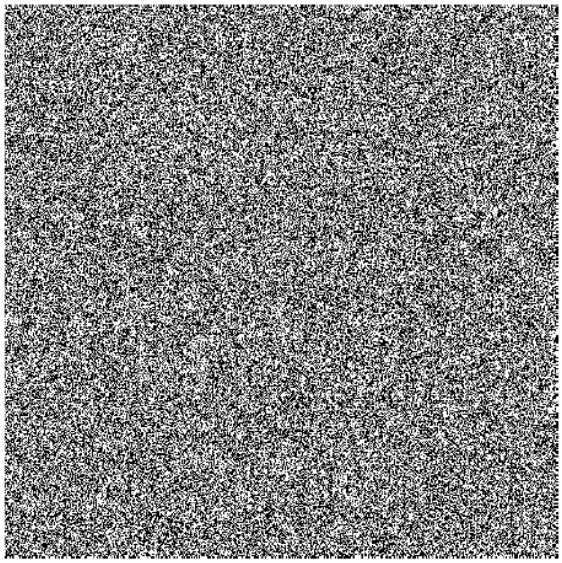


Figure 6: *Histogram of a random picked block of numbers the size of 100000 uint8 values.*

Histogram liczb uzyskanych poprzez konwersję ciągu bitów na ciąg liczb uint8



Rys. 7. Bitmapa (512 x 512 pikseli) losowo wybranych przykładowych danych.

Dane, które przejdą ten test można uważać za losowe. Niestety, duży zestaw liczb przeszedł jedynie 3 testy (por. Tabela I).

---

[6] John von Neumann, "Various techniques used in connection with random digits," in A.S. Householder, G.E. Forsythe, and H.H. Germond, eds., *Monte Carlo Method*, National Bureau of Standards Applied Mathematics Series, 12 (Washington, D.C.: U.S. Government Printing Office, 1951): 36-38.

[7] Robert G. Brown, Dirk Eddelbuettel, David Bauer. Dieharder: A Random Number Test Suite, Duke University Physics Department, Durham. https://webhome.phy.duke.edu/~rgb/General/dieharder.php

Tabela I. Wyniki trzech testów DieHardera dla wybranego losowo zestawu bitów.

```
$ dieharder -a -g 201 -f random0_tmpcpy1.bin
#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|     random0_tmpcpy1.bin        |  3.11e+07  |
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
   diehard_birthdays|  0|       100|     100|0.82076730|  PASSED
      diehard_operm5|  0|   1000000|     100|0.50891570|  PASSED
  diehard_rank_32x32|  0|     40000|     100|0.67785857|  PASSED
```

Wnioski:

Jak wynika z przeprowadzanego testu, generowany ciąg nie jest losowy nawet po usunięciu „bias-u". Powodem może być udział szumu $1/f$ dla ciągu zbieranego w dłuższym czasie oraz deterministyczny szum termiczny. W związku z powyższym planowana jest stosowna modyfikacja zaproponowanego rozwiązania. Ponadto planuje się również zastosowanie innych metod usunięcia „bias"-u[8]. Należy zaznaczyć, że zaproponowane rozwiązanie jest atrakcyjne ze względu na gabaryty i możliwość integracji z krzemową elektroniką co potencjalnie może skutkować dalszą miniaturyzacją.

II. Generator liczb losowych oparty na szumie śrutowym. Wersja II.

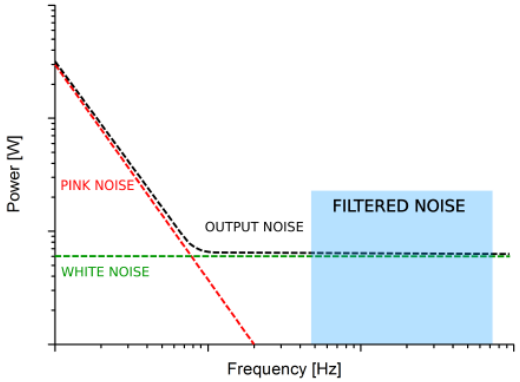
W kolejnej wersji generatora opartej na szumie śrutowym zaproponowano układ gwarantujący odseparowanie kwantowego szumu śrutowego od pozostałych źródeł szumu.

W tym rozwiązaniu zamiast szumu związanego z efektem Zenera, zastosowano szum generowany przez fotodiodę oświetlaną światłem emitowanym przez diodę elektroluminescencyjną.

Szum generowany przez urządzenie półprzewodnikowe może być podzielony na dwie klasy ze względu na spektrum częstotliwości, f. Są to: szum różowy, którego spektrum jest proporcjonalne do $1/f$ oraz szum biały, którego spektrum nie zależy od f.

W skład szumu białego wchodzą szum śrutowy oraz szum termiczny. Jeśli uda się usunąć szum różowy (np. przy użyciu odpowiednich filtrów górnoprzepustowych) otrzyma się tylko szum biały (por. rys. 8). Z kolei odseparowanie szumu śrutowego jest możliwe stosując komparatory okna.

[8] Boaz Barak, Ronen Shaltiel, Eran Tromer. True Random Number Generators Secure in a Changing Environment, In Workshop on Cryptographic Hardware and Embedded Systems (CHES), of LNCS, pp. 166-180, 2003.



Rys. 8. Spektrum częstotliwościowe szumów w urządzeniach półprzewodnikowych.

Szczegółowy opis zaproponowanego rozwiązania wraz z uzyskanymi wynikami testu NIST przeprowadzonego na losowo wybranym zestawie bitów przedstawiono w następujących załącznikach:

1. Wersja robocza pracy przygotowywanej do publikacji (J. Niemczuk „Random Quantum Noise Generation Using Shot Noise In Semiconductors")

2. Prezentacja posterowa, która została przedstawiona podczas Krajowej Konferencji Elektroniki, Darłówko Wschodnie 3.06-07.06 2018.

3. Kopia wyróżnienia ww. prezentacji przez Komitet Naukowy w ramach konkursu „Młodzi pracownicy nauki"

4. Prezentacja konferencyjna na 1st International Symposium on Quantum Technology, 24-27 June 2018, Aberdeen UK (oral) (J. Niemczuk, E. Popko, S. Drobczyński and T. Martynkien „Cryptographic Quantum Random Number Generation Using Shot Noise"

III. **Układ akwizycji danych dla kwantowych generatorów liczby losowych.**

Drugie podejście do wykonania zadań w ramach niniejszej umowy, dotyczy opracowania uniwersalnej platformy akwizycji danych, która może współpracować z różnymi układami kwantowych generatorów liczby losowych. Układ elektroniczny ma być kompaktowy, zasilany bateryjnie oraz charakteryzować się możliwością szybkiego próbkowania sygnałów analogowych i cyfrowych.

Sygnały wejściowe pochodzące z różnych źródeł entropii, można podzielić na dwie kategorie:

- sygnał cyfrowy np. z liczników pojedynczych fotonów; jest to na ogół sygnał w standardzie TTL o częstotliwości 100-150 MHz.
- szerokopasmowy analogowy sygnał szumu.

Koncepcją projektowanego systemu jest skupienie układów peryferyjnych wokół jednostki logicznej typu FPGA (ang. *F*ield-Programmable Gate Array). Technologia FPGA pozwala na bardzo szybkie komunikowanie układów peryferyjnych co z kolei przekłada się na duże prędkości próbkowania sygnału i transfer danych. Urządzenie wyposażone jest w dwa niezależne kanały wejściowe a dzięki możliwościom układu FPGA sygnały wejściowe będą próbkowane jednocześnie. Aby zwiększyć uniwersalność urządzenia na złączu szpilkowym udostępnione zostaną wejścia przetworników analogowo-cyfrowych oraz porty I/O układu FPGA. To rozwiązanie umożliwi dołączanie wyspecjalizowanych modułów formujących sygnały wejściowe.

Na rys. 9 przedstawiono zdjęcie układu pomiarowego, który jest w trakcie realizacji. Został on wyposażony w wyspecjalizowany rejestrator analogowo-cyfrowy. Rejestrator zbudowany jest z szybkich przetworników analogowo-cyfrowych, układu FPGA, pamięci RAM oraz mikrokontrolera z rdzeniem ARM do szybkiej transmisji danych. Dokładny opis architektury układu przedstawiono w załącznikach 5 i 6.

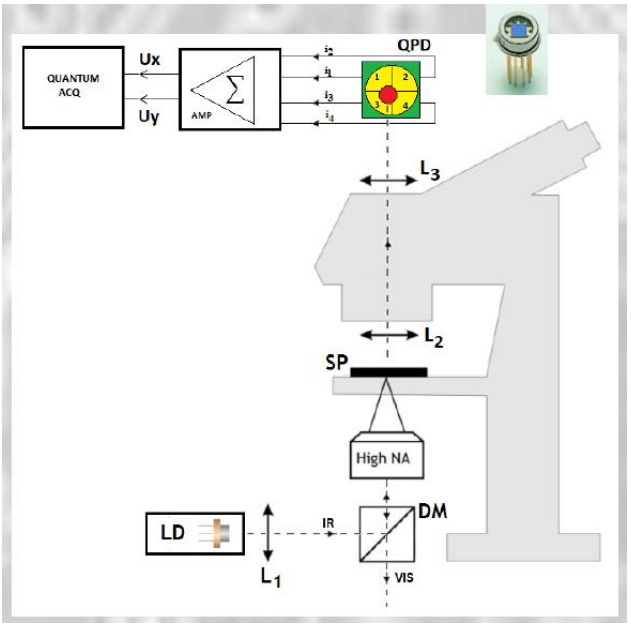
Rys. 9. Układ do akwizycji danych dla kwantowych generatorów liczby losowych

W celu przetestowania układu akwizycji danych zostanie on wykorzystany do rejestracji sygnału szumu śrutowego na wyjściu fotodiody (z układu przedstawionego w załącznikach 2 i 4) oraz drgań polistyrenowej mikro-kulki uwięzionej w pułapce optycznej. Jej drgania wokół położenia równowagi spowodowane są zderzeniami z cząsteczkami cieczy, w której się znajduje. Układ umożliwi rejestrację sygnału drgań i zbadanie kwantowej natury ruchów Browna cząsteczek cieczy.

Zjawisko pułapkowania optycznego obserwujemy dla niewielkich obiektów dielektrycznych umieszczonych w silnie zogniskowanej wiązce laserowej. Trójwymiarowe pułapkowanie jest wynikiem dominacji siły pochodzącej od wzajemnego odziaływania składowej elektrycznej wiązki światła oraz indukowanego dipola elektrycznego nad siłą powstającą w skutek przekazania pędu przez rozproszone fotony. Dla niewielkich wychyleń obiektu z położenia równowagi potencjał pułapki optycznej można przybliżyć potencjałem harmonicznym. Ruch pułapkowanej cząstki w potencjale harmonicznym opisuje równanie

Langevina uwzględniające tłumienie ośrodka oraz wymuszenie pochodzące od zderzeń pułapkowanego obiektu z cząsteczkami cieczy, w której się znajduje. Rozwiązaniem równania ruchu jest proces Ornsteina-Uhlenbecka, który charakteryzuje się tym, że aktualna wartość jest kombinacją liniową wartości poprzedniej i zewnętrznego szumu. Ten szum drgań pułapkowanego obiektu jest źródłem losowego ciągu liczbowego.

Rys. 10 przedstawia schemat zaprojektowanego układu optycznego. Układ jest w trakcie realizacji.



Rys. 10 Układ optyczny pułapki optycznej

Szczegółowy opis zaproponowanego rozwiązania przedstawiono w następujących załącznikach:

- Publikacja „Układ akwizycji danych dla kwantowych generatorów liczby losowych.”
- Prezentacja konferencyjna na Krajowej Konferencji Elektroniki, Darłówko Wschodnie “Zastosowanie pułapki optycznej do generatora liczb losowych”.