1. Marek LEŚNIEWICZ, 2. Piotr KOMOROWSKI, 3. Janusz ZABŁOCKI

Wojskowy Instytut Łączności – Państwowy Instytut Badawczy
ORCID: 1. 0000-0001-5505-1268; 2. 0000-0002-0752-0055; 3. **0000-0001-5429-8058**

doi: 10.15199/48.2023.04.35

Analiza możliwości sprzętowej generacji losowych ciągów binarnych z przepływnością 1 Gbit/s

Streszczenie. *W artykule przedstawiono analizę możliwości sprzętowej generacji doskonale losowych ciągów binarnych z przepływnością 1 Gbit/s, wykorzystującą układy i sygnały mikrofalowe. W analizie użyto powszechnie znanych modeli generacji ciągów losowych, jednak z wykorzystaniem niestosowanych dotąd w tym celu technologii, w tym zastosowania do kreacji ciągów układów programowalnych FPGA. Analizy udokumentowano wynikami pomiarów rzeczywistych układów i sygnałów w funkcji czasu i częstotliwości za pomocą oscyloskopu i analizatora widma w paśmie 2 GHz.*

Abstract*. The article presents an analysis of the hardware capabilities of generating truly random binary strings with a bit rate of 1 Gbps, using microwave circuits and signals. The analysis uses commonly known models of random sequence generation, but with the use of technologies that have not been used for this purpose so far, including the use of FPGA programmable circuits for the creation of sequences. The analyzes were documented with the results of measurements of real systems and signals as a function of time and frequency using an oscilloscope and a spectrum analyzer in the 2 GHz band.* (***Analysis of the hardware capabilities of the generation of random binary sequences with a bit rate of 1 Gbps.***)

Słowa kluczowe: generacja ciągów (liczb) losowych, losowość, entropia, układy i sygnały mikrofalowe
Keywords: random sequences (number) generation, randomness, entropy, microwave circuits and signals

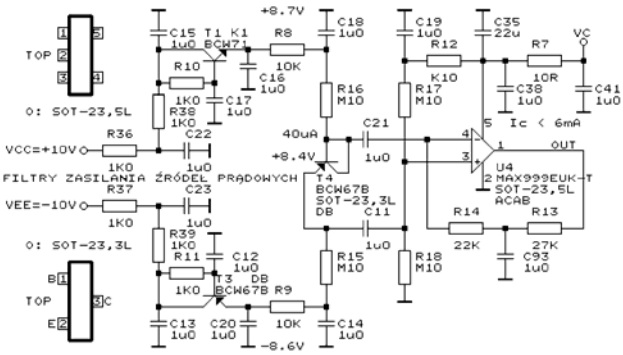
Wstęp

Przedmiotem pracy jest analiza możliwości sprzętowej generacji doskonale losowych ciągów binarnych o jednostkowej entropii z przepływnością 1 Gbit/s. Ciągi te mają liczne i ważne zastosowania w wielu dziedzinach nauki i techniki, ze wskazaniem na kryptografię, statystykę, obliczenia numeryczne, cyfrowe przetwarzanie sygnałów, symulacje stochastyczne, algorytmy randomizowane i in. [1]

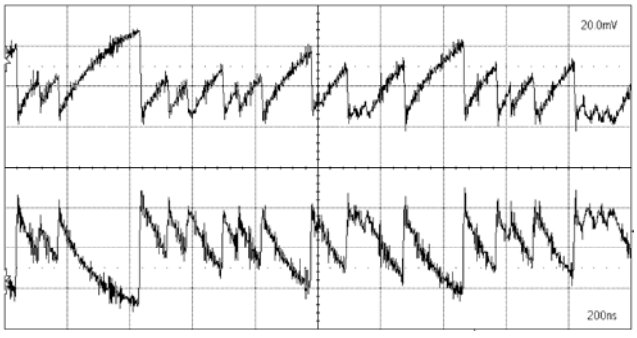
W zastosowaniach tych używa się obecnie wyłącznie ciągów właśnie prawdziwie losowych, tzn. pochodzących ze źródeł w postaci generatorów sprzętowych TRNG (*True Random Number Generator*) [1, 2]. Ich typowe rozwiązania umożliwiają wytwarzanie ciągów o przepływnościach do 10 Mbit/s, tymczasem indywidualne potrzeby współczesnych urządzeń i aplikacji sięgają już nawet 1 Gbit/s.

Propozycją generatora o bardzo dużej przepływności może być rozwiązanie, opisane w [3]. Ciągi uzyskiwane w układzie wykorzystującym opisaną tam metodę mają referencyjne właściwości i parametry statystyczne, mogą więc być użyte w wielu zastosowaniach naukowych. Jednak w przypadku kryptografii za bezpieczne uznaje rozwiązania oparte wyłącznie na analitycznie okazanej i praktycznie zmierzonej źródłowej entropii, tzn. bez jej przetwarzania, czy zwłaszcza „poprawiania" w układach algorytmicznych.

Około roku 2005 w Wojskowym Instytucie Łączności opracowano sprzętowy generator ciągów losowych SGCL o przepływności 8 Mbit/s [2], który uzyskał certyfikat Służby Kontrwywiadu Wojskowego do ochrony informacji o klauzuli *ściśle tajne*. Generator ten posiadał matematyczny dowód bezpieczeństwa oparty nie na badaniach statystycznych, ale właśnie na analizie i pomiarach entropii. Dzięki temu generował ciągi o gwarantowanej entropii, spełniające w dowolnej próbie wszystkie znane testy statystyczne na referencyjnym poziomie losowości. Jego konstrukcja i wdrożenie w tamtych czasach były możliwe nie tylko dzięki temu dowodowi, ale przede wszystkim pojawieniu się nowoczesnych układów programowalnych FPGA o nowych, unikatowych właściwościach i parametrach elektrycznych. Dotyczyły one głównie szybkości przetwarzania sygnałów losowych, modelowanych jako asynchroniczne sygnały Poissona [4]. Źródłem tych sygnałów były diody lawinowe, wykorzystujące zjawisko mikroplazmatycznego przebicia złącza p-n, pracującego w trybie odwrotnej polaryzacji. Rozwiązanie to nie zestarzało się w sensie technicznym, ponieważ dostępne dzisiaj diody lawinowe nie mają znacząco lepszych właściwości i parametrów w sensie widmowym, które są ograniczone częstotliwością 100 MHz, a układy programowalne ogólnego przeznaczenia nie dysponują możliwościami wprowadzania i przetwarzania sygnałów o częstotliwościach większych od 150 MHz. Typowy układ przetwarzania takich sygnałów ze złącza p-n tranzystora T4 przez komparator U4 przedstawia rysunek 1 (fragment konstrukcji generatora SGCL [2]), a przebiegi czasowe na wejściach i wyjściu komparatora rysunki 2 i 3.



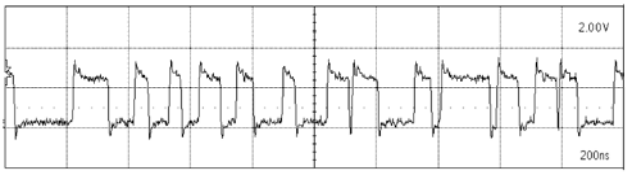
Rys.1. Układ referencyjnego generatora sygnału Poissona [2]



Rys.2. Typowe, źródłowe sygnały Poissona z obu końcówek diody lawinowej – napięcia międzyszczytowe są rzędu 10÷20 mV_{PP}

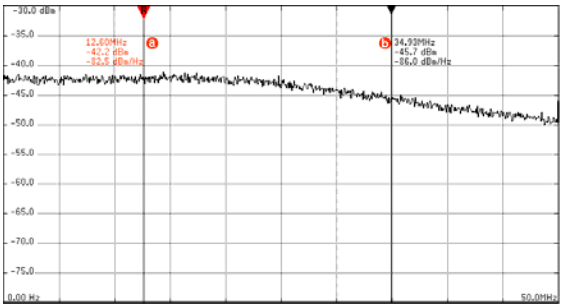
Minimalna gęstość zmian sygnału Poissona z takiego złącza, po starannym wyborze punktu pracy w sensie prądu złącza p-n, wynosi $\lambda > 20$ MHz, a jego funkcja autokorelacji dana jest jako $K = \exp(-2\lambda / f_P)$, gdzie $f_P = 8$ MHz jest typową częstotliwością próbkowania. Po próbkowaniu takiego sygnału uzyskuje się zrównoważony, losowy ciąg

binarny o korelacjach międzyelementowych $K < 10^{-2}$, a stąd entropię ciągu liczoną na 1 element nie mniejszą niż $H > 0{,}99996$ bit/e. Wartość ta nie jest jeszcze zadowalająca, ale już rokuje otrzymanie wynikowych ciągów o właściwościach i parametrach uznawanych za doskonale losowe.



Rys.3. Sygnał Poissona na wyjściu komparatora (nie jest to wynik komparacji tej samej sekwencji, co na rysunku 2) – po komparacji napięcia wyjściowe przyjmują binarne wartości 0 V i 3,3 V

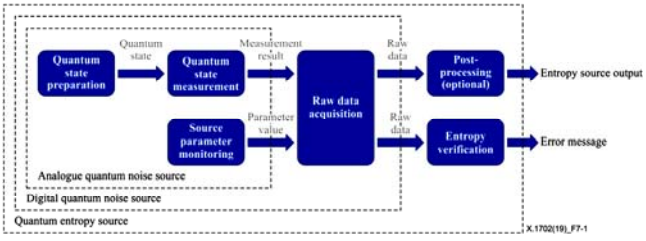
Powyższą analizę należy uzupełnić o widmowe właściwości i parametry sygnału Poissona. Łatwo wykazać, że sygnał o funkcji autokorelacji postaci $K(\tau) = \exp(-2\lambda|\tau|)$ charakteryzuje widmowa gęstość mocy $G(\omega) = G(0) / \{1 + (\omega / 4\lambda)^2\}$, co dla sygnału z rysunku 3 o gęstości zmian λ = 40 MHz i częstotliwości f_{BW} = 35 MHz punktu 3 dB spadku wartości funkcji $G(\omega)$, ilustruje rysunek 4. Ze wzorów i pomiarów wynika, że $\omega_{BW} = 4\lambda = 2\pi f_{BW}$, a więc $\lambda = \pi/2\, f_{BW}$. Jeśli przyjąć, że w odpowiednio długim okresie czasu $\lambda = 2 f_{ŚR}$, tzn. że połowa zmian w sygnale Poissona odpowiada jego umownej, średniej częstotliwości $f_{ŚR}$, to $f_{ŚR} = \pi/4\, f_{BW}$. Jeśli sygnał jest rzeczywiście Poissona, a jego widmo opisane funkcją $G(\omega)$ zostało zweryfikowane pomiarowo, jak na rysunku 4, to uwzględniając jego losowy charakter, przy odpowiednio długich czasach pomiarów poprawność powyższych zależności jest zgodna z dokładnością do 20%, nawet dla częstotliwości f_{BW} przekraczających 1 GHz.



Rys.4. Widmowa gęstość mocy sygnału Poissona o λ = 40 MHz

Łatwo teraz zauważyć, że generacja ciągów o przepływności 1 Gbit/s będzie wymagała źródeł sygnałów około 100-krotnie szybszych i układów je przetwarzających działających w paśmie co najmniej kilku GHz.

Na rysunku 5 przedstawiono typowy, uznany schemat blokowy generatora ciągów losowych, taki sam niezależnie od konstrukcji i szybkości generowanych ciągów, cytowany z dokumentu ITU-T [5]. Według takiego samego schematu był skonstruowany również generator WIŁ z roku 2005.



Rys.5. Układ referencyjnego generatora ciągów losowych [5]

Dokument ten opisuje perspektywiczny generator ciągów prawdziwie losowych, jednak bez specyfikacji technicznej w sensie realizowalności, czy wymaganej szybkości generacji. Z treści dokumentu wynika, że jest to kolejne, zupełnie odmienne podejście do konstrukcji generatora ciągów prawdziwie losowych w sensie źródła losowości, jako że dotychczasowe były zdecydowanie nieudane. Dotyczy to zwłaszcza konstrukcji opartych na wykorzystaniu pozornie losowych właściwości układów programowalnych FPGA, takich jak metastabilność itp. [6]. „Nieudane" oznacza w tym przypadku konstrukcje generujące ciągi „wyglądające jak losowe" (*looks like random*), jednak o nieudowodnionej losowości, bez mechanizmów kontroli entropii i zwykle niespełniające nawet podstawowych testów statystycznych.

Używane w nim pojęcie źródła kwantowego nie oznacza źródła światła, a ogólnie rozumiane źródła, podlegające prawom fizyki kwantowej, z tak odmiennymi przykładami, jak superpozycja stanów kwantowych, splątanie stanów kwantowych, tunelowanie kwantowe, emisja spontaniczna czy rozpad radioaktywny [1], [7]. Schemat ten nie opisuje jednak technologii przetwarzania kwantowych *parametrów* takich nanoskopowych źródeł, ponieważ nie są znane takie przetworniki. Tym samym niewyobrażalne byłyby badania, czy pomiary rzeczywistej entropii takich zjawisk na poziomie pojedynczych kwantów, czy cząstek. Nawiązując do układu z rysunku 5 można też zauważyć, że pojedynczy kwant, czy cząstka odebrane i użyte do generacji ciągu operacyjnego nie mogą być przecież powtórnie użyte do testu entropii i odwrotnie. W praktyce twierdzenie, że fizyka kwantowa teoretycznie dowodzi źródłowej losowości stanu takich nanoskopowych zjawisk nie oznacza, że ta losowość jest również właściwością ciągu zdarzeń w rzeczywistych, fizycznych warunkach, np. w sensie technicznego odbioru strumieni kwantów, czy cząstek [1], [7]. Znane rozwiązania wykorzystują zatem wtórnie kwantowe *właściwości* takich zjawisk, np. optycznej filtracji i detekcji fotonów o polaryzacji pionowej i poziomej, na razie z niską i niestabilną w czasie dokładnością rzędu 5%. Trudno powiedzieć, czy zmienność tych zjawisk byłaby opisywana częstością zdarzeń rzędu miliardów na sekundę, by osiągnąć pożądaną przepływność 1 Gbit/s. W cytowanych publikacjach [1], [7] dowodzi się na bardzo różnych przykładach eksperymentalnych, że osiąga się od zaledwie kilku bit/s do co najwyżej kilku Mbit/s.

Trzeba też pamiętać, że każde urządzenie techniczne podlega różnym wymaganiom eksploatacyjnym, związanym z mechanicznymi, klimatycznymi i elektromagnetycznymi warunkami pracy. Urządzeniom elektronicznym stawia się wysokie wymagania w sensie odporności w czasie pracy na narażenia klimatyczne w założonym przedziale temperatur i wilgotności oraz narażenia mechaniczne. Ponadto wymaga się poprawnej pracy urządzenia w zakłóconym środowisku elektromagnetycznym, ale jednocześnie braku wpływu tego urządzenia na zakłócanie tego środowiska. Trudno byłoby powiedzieć, jak w tych warunkach wyglądałyby praca i spełnienie takich wymagań przez np. przenośny generator, wykorzystujący zjawisko rozpadu radioaktywnego.

Dlatego, zdaniem autorów, mówiąc o perspektywicznym generatorze o wyjściowej przepływności 1 Gbit/s, należy przyjmując schemat realizacji z rysunku 5, zastosować dzisiaj najnowsze rozwiązania z dziedziny mikrofalowych źródeł szumów i wybranych, specjalizowanych układów programowalnych FPGA, zdolnych do przyjmowania i przetwarzania sygnałów w paśmie rzędu kilku GHz.

Konstrukcja generatora szumu mikrofalowego

Generatory szumów mikrofalowych są podstawowym źródłem do badań większości obiektów przetwarzających sygnały elektryczne i radiowe w paśmie powyżej 300 MHz. Dotyczy to tak różnych urządzeń jak anteny, filtry, tłumiki,

sprzęgacze, dzielniki, czy odbiorniki i nadajniki mikrofalowe. Lista producentów takich generatorów nie jest zbyt długa (Keysight, Noisecom, Noisewave i in.), a lista oferowanych produktów liczy w każdej z firm po kilkanaście pozycji. Są to zasadniczo generatory addytywnych białych szumów gaussowskich AWGN (*Additive White Gaussian Noise*), a ich podstawowe właściwości i parametry są następujące [8]:

- szerokość widma BW (*bandwidh*), od 1 GHz do 50 GHz,
- względny poziom widmowej gęstości mocy ENR (*Excess Noise Ratio*) ponad poziomem szumu odniesienia, od 30 dB do 50 dB, w wybranych modelach do nawet 65 dB,
- nierównomierność funkcji widmowej gęstości mocy (*ENR uncertainty*), zwykle od ułamka dB do kilku dB.

Przesyłając sygnały z takich generatorów na większe odległości dla konkretnych typów kabli i złączy określa się ponadto współczynnik fali stojącej SWR (*Standing Wave Ratio*) oraz współczynnik odbicia Γ (*Reflection Coefficient*).

Konkretne rozwiązania techniczne takich generatorów są dość zróżnicowane [8] – od dużych modułów o wymiarach sięgających kilkunastu cm, poprzez obudowy zbliżone wymiarami do typowych, przewlekanych DIP-14/DIP-24, po okrągłe, 4-końcówkowe obudowy TO-8 o średnicy 1/2 cala. Zakup takich elementów nie jest jednak ani prosty, ani tani, stąd warto dzisiaj rozważyć własną konstrukcję.

Propozycja wynika z dwóch przesłanek:

- własna konstrukcja uniezależnia od rynku, kosztów i narzuconych rozwiązań konstrukcyjnych, zwłaszcza wymiarów mechanicznych i interfejsów elektrycznych,
- oferta elementów do własnej konstrukcji jest dzisiaj na tyle szeroka i tania, że warto spróbować opracować rozwiązanie może nie lepsze, ale parametrycznie choćby porównywalne, za to ściśle dopasowane konstrukcyjne do własnych potrzeb.

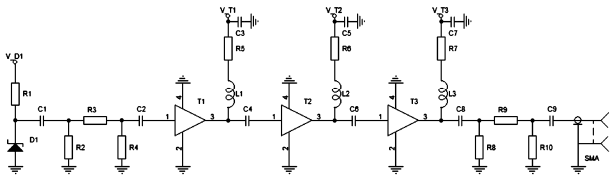
Wstępne założenia do takiej konstrukcji są następujące:

- źródłem szumu będzie mikrofalowa dioda lawinowa, generująca szum w paśmie kilku GHz,
- szum ten musi zostać wzmocniony bez zniekształceń źródłowego widma do poziomu, który pozwoli na wprowadzenie go bezpośrednio na specjalizowane wejścia odbiornika transcivera układu programowalnego FPGA, mającego zdolność odbierania asynchronicznych sygnałów binarnych, modelowanych jako sygnały Poissona i próbkowania ich z częstotliwością do 10 GHz,
- przy takich założeniach poziom napięciowy sygnału po wzmocnieniu powinien sięgać 1 V_{PP}, a więc jego moc na obciążeniu 50 Ω może wynosić do 7 dBm.

Konstrukcja takiego układu jest znana, nieskomplikowana, ale jej realizacja wymaga głębokiej wiedzy i doświadczenia w zakresie projektowania i badania układów mikrofalowych oraz zwykle kilku kolejnych projektów płytek drukowanych, zanim osiągnie się w pełni zadawalające wyniki [9].

Przykładowy układ, przedstawiony na rysunku 6, zawiera:

- mikrofalową diodę lawinową D1 z układem dopasowania,
- trójstopniowy układ wzmacniający T1, T2, T3,
- wyjściowy układ dopasowania,
- obwody zasilania i ustawiania punktów pracy T1, T2, T3.



Rys.6. Układ mikrofalowego generatora sygnału Poissona

Pierwszym założeniem do konstrukcji są jak najszersze widmo szumu z diody lawinowej i jak najszersze pasmo przenoszenia układu wzmacniającego. Założenie wynika z intencji osiągnięcia wyjściowego sygnału modelowanego jako sygnał Poissona o jak największej gęstość zmian, a wiec siłą rzeczy jak najszerszym widmie sygnału wyjściowego. Drugim założeniem jest prostota układowa, sprowadzająca się do możliwości powielania sprawdzonego układu o bezwarunkowej stabilności i stałym wzmocnieniu w całym paśmie oraz znormalizowanym poziomie sygnału wyjściowego, dopasowanym do czułości wejść odbiorników transceiverów układu programowalnego.

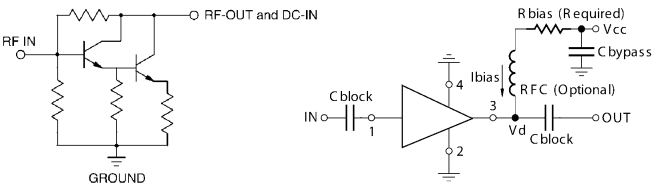
Typowe właściwości i parametry szumów z lawinowych diod mikrofalowych [8], również wykorzystujących zjawisko mikroplazmatycznego przebicia złącza p-n, są następujące:

- szerokość widma BW do 10 GHz,
- praca na obciążeniu 50 Ω,
- względny poziom widmowej gęstości mocy ENR od 30 dB do 35 dB,
- napięcie pracy od 8 V do 12 V przy optymalnym prądzie złącza p-n od 8 mA do 10 mA,
- możliwość powiększenia szerokości widma BW do nawet 50 GHz, jednak kosztem dużego spadku względnego poziomu widmowej gęstości mocy ENR o około 10÷15 dB, co jednak nie ma uzasadnienia wobec niemożności wprowadzenia i przetwarzania tak szybkich sygnałów w układach programowalnych oraz komplikacji konstrukcji wzmacniaczy pracujących w tak szerokim paśmie.

Do konstrukcji wzmacniacza można użyć szerokiej gamy układów mikrofalowych MMIC (*Monolithic Microwave Integrated Circuit*), które można traktować i implementować jako gotowe, zintegrowane wzmacniacze o następujących, przykładowych właściwościach i parametrach [10]:

- pasmo przenoszenia od prądu stałego do nawet 8 GHz,
- wejścia i wyjścia wewnętrznie dopasowane do pracy z obciążeniami 50 Ω,
- bezwarunkowa stabilność,
- wzmocnienie bazowe dla małych częstotliwości od 10 dB do 20 dB, ale spadek wzmocnienia dla częstotliwości granicznych na końcu pasma przenoszenia wynosi typowe 3 dB,
- duży zakres dynamiki wzmacnianych sygnałów – moce, przy których następuje nieliniowe ograniczanie sygnałów wyjściowych (*saturated output power compression*), to od 5 dBm do 20 dBm,
- współczynnik szumów NF nie większy niż 5 dB, ale w specjalizowanych modelach nie przekracza nawet 1 dB,
- typowe napięcie pracy 5 V przy prądzie od 50 mA do 100 mA, a więc mocy strat od 250 mW do nawet 500 mW,
- 4-końcówkowe obudowy zdolne do odprowadzania takich mocy przy typowej temperaturze pracy sięgającej +60^{O}C.

Na rysunku 7 przedstawiono wewnętrzny i aplikacyjny schemat przykładowego układu MMIC typu ERA-1+.

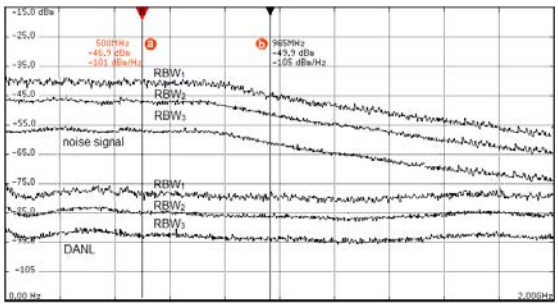


Rys.7. Schemat wewnętrzny i aplikacyjny układu MMIC [10]

Wyniki badań generatora szumu mikrofalowego

Na rysunku 8 przedstawiono wyniki działania układu z rysunku 6 w sensie bezwzględnego poziomu wyjściowej widmowej gęstości mocy w paśmie 2 GHz na wyjściu obciążonym rezystancją 50 Ω. Pomiary uzupełniono poziomami szumów odniesienia DANL, co pozwoliło na wyznaczenie współczynników ENR o zmiennych, tzn. malejących w funkcji częstotliwości, w każdym przypadku

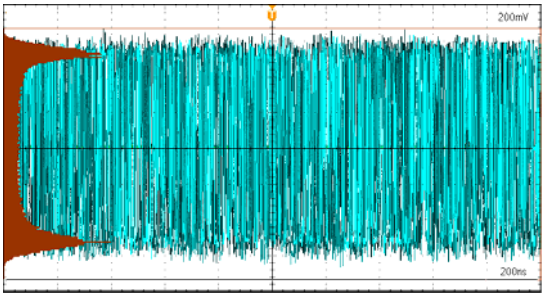
relatywnie dużych wartościach od 40 dB do 20 dB. Badanie przeprowadzono z zastosowaniem trzech opcji filtru pomiarowego – w paśmie RBW_1 = 2 MHz, RBW_2 = 200 kHz i RBW_3 = 20 kHz. Stosunek szerokości tych pasm wynosi 10, więc poziom szumu odniesienia obniża się o ok. 10 dB. O taką samą wartość obniża się również poziom wyjściowej widmowej gęstości mocy, co jest pozornie sprzeczne z praktyką pomiarową sygnałów deterministycznych, których poziomy są zachowywane niezależnie od szerokości filtrów pomiarowych, a jedynie lepiej obrazowane przy ich zawężaniu. W tym przypadku dany jest jednak sygnał, który jest przetwarzany jako sygnał szumowy i podlega takiej właśnie obróbce, niezależnie od swojego poziomu. Funkcja widmowej gęstości mocy opisana jest jako $G(\omega) = G(0) / \{1 + (\omega/4\lambda)^2\}$, gdzie $\lambda = \pi/2\ f_{BW}$ = 1,5 GHz, sygnał ten odpowiada zatem modelowi sygnału Poissona. Najważniejszym spostrzeżeniem jest jednak, że obwiednia tak szerokiego widma nie zawiera nierównomierności, czy prążków, stąd taki sygnał można uznać za w pełni losowy.



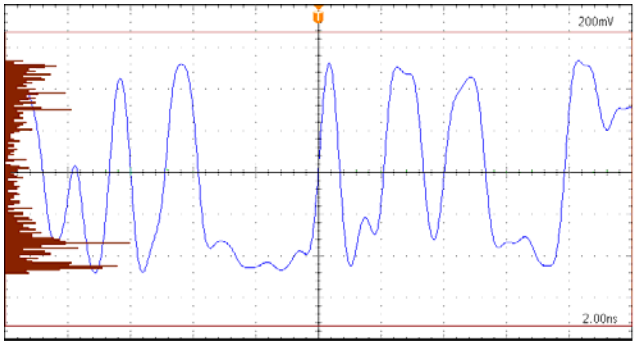
Rys.8. Widmowe gęstości mocy i szumy odniesienia w pasmach pomiarowych RBW_1 = 2 MHz, RBW_2 = 200 kHz i RBW_3 = 20 kHz

Równie interesujące są przedstawione na rysunkach 9 i 10 oscylogramy sygnału wyjściowego układu z rysunku 6 w sensie przebiegów czasowych i równomiernego rozkładu gęstości prawdopodobieństwa wartości sygnału na wyjściu obciążonym rezystancją 50 Ω. Widać na nich sygnały o wartości międzyszczytowej 0,8 V_{PP}, a więc mocy na obciążeniu 50 Ω równej 5 dBm. Przebiegi sygnałów mają referencyjne kształty sygnału Poissona. Rozkład gęstości prawdopodobieństwa wartości sygnałów składa się z trzech części, odpowiadających za realizacje na poziomie +0,4 V, –0,4 V i w strefie przejściowej między tymi wartościami. Strefa przejściowa ma rozkład praktycznie równomierny, co wskazuje, że sygnał nie przyjmuje w niej wartości pośrednich, a jedynie „przebywa" tam między zmianami od +0,4 V do –0,4 V i odwrotnie. Pewien wpływ na czas tego przebywania ma niezerowy czas narastania i opadania sygnału, wynikający z ograniczenia pasma przenoszenia obwodów wejściowych oscyloskopu, równego BW = 1 GHz. Z tego względu szybkie realizacje spoza tego pasma nie są prezentowane w pełnym zakresie zmienności od +0,4 V do –0,4 V i odwrotnie, ale w rzeczywistości tak właśnie zmienia się ten przebieg. Czy te właściwości zostały przeniesione ze źródłowego sygnału z diody lawinowej, czy są wynikiem nieliniowego ograniczania w układzie wzmacniającym z rysunku 6? Z analiz wynika, że ograniczanie następuje dopiero w ostatnim stopniu T3, ale odpowiedź na to pytanie nie może być potwierdzona pomiarowo. Sygnał szumu z diody ma poziom 1 mV_{SK}, dający się zatem zmierzyć, ale nie monitorować oscyloskopem, zaś próby obserwacji oscyloskopowych wewnątrz układu wprowadzają do niego silne zakłócenia i powodują wynikowy stan niestabilności.

Obserwacje te potwierdzają istotę właściwości λ, parametru sygnału Poissona, który stanowi nie tylko jego wartość oczekiwaną i ale i wariancję [4]. Z oscylogramów widać, że wartość oczekiwana jest stała, zaś odchylenie standardowe $\sqrt{\lambda}$ jest niewielkie, dla λ = 1,5 GHz zaledwie $\sqrt{\lambda}$ = 39 kHz.



Rys.9. Sygnał Poissona na wyjściu układu generatora w przedziale czasu 400 ns – napięcia przyjmują binarne wartości +0,4 V i –0,4 V a funkcja gęstości prawdopodobieństwa jest ustabilizowana



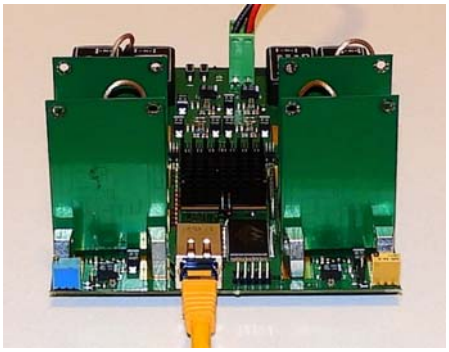
Rys.10.Sygnał Poissona na wyjściu układu generatora w przedziale czasu 20 ns – napięcia przyjmują binarne wartości +0,4 V i –0,4 V, funkcja gęstości prawdopodobieństwa reprezentuje tylko 30 zmian sygnału, co pozwala jednak ponownie oszacować λ = 1,5 GHz

Analiza możliwości zastosowania transceivera układu FPGA, jako kreatora binarnego ciągu losowego

W zaawansowanych wersjach układów programowalnych FPGA są do dyspozycji specjalizowane transceivery do transmisji szeregowej z przepływnościami do 12 Gbit/s [11]. Transmisje te mają bardzo różne opcje w sensie organizacji ramkowej (*framed*), i mogą obsługiwać tak różne interfejsy cyfrowe jak Ethernet, PCIe, SATA, HDMI, DisplayPort i wiele innych. Idea użycia takiego tranceivera polega na fizycznym, elektrycznym dopasowaniu sygnałów do jego wejść i wyjść oraz na użyciu wewnątrz układu FPGA odpowiedniego komponentu programowego, obsługującego logicznie dany interfejs. Doświadczenia aplikacyjne autorów z takimi interfejsami są pozytywne. Po prostu należy ściśle przestrzegać zaleceń producenta danego układu FPGA, a w konstrukcji samych interfejsów używać standardowych modułów w sensie np. transceiverów elektrooptycznych 10 Gbit/s SFP+ (*Small Form-factor Pluggable 10Gbps*), czy specjalizowanych złączy elektrycznych PCIe, SATA itp., by osiągnąć poprawne wyniki użytkowe. Okazuje się, że przy odpowiednio, tzn. właściwie i bardzo krótko prowadzonych ścieżkach w sensie linii paskowych, do konstrukcji układów pracujących nawet z przepływnością 10 Gbit/s wystarczy zastosowanie standardowego laminatu klasy FR4 [9], [11].

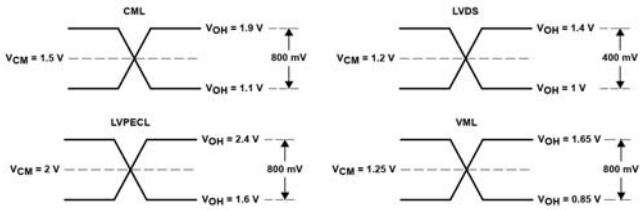
Do dalszych prac użyto układów programowalnych firmy INTEL rodziny ARRIA V GT typu 5AGTMC7G3F31I3N [11|. Wynikało to stąd, że autorzy mieli już doświadczenia z tymi układami, zdobyte w czasie prac nad interfejsami Ethernet 10GBase-FX i optoelektronicznymi modułami SFP+. Na ich podstawie zaprojektowano układ generatora, przedstawiony na rysunku 11. Zawiera on 4 mikrofalowe generatory składowe, moduł zasilania oraz interfejsy Ethernet

1000Base-TX i USB 2.0 HS. Dzięki optymalizacji połączeń wewnętrznych płytka drukowana jest tylko 6-warstwowa.



Rys.11. Układ mikrofalowego generatora ciągów losowych

Sygnały o takich przebiegach wartości napięć, jak na rysunkach 9 i 10, dają się łatwo wprowadzić na 50 Ω, standardowe wejścia odbiorników transciverów układu FPGA. Na rysunku 12 przedstawiono wymagania dla poziomów napięć wejściowych standardowych odbiorników. Widać, że najczęściej spotykanym jest właśnie poziom od +0,4 V do –0,4 V względem stałego napięcia odniesienia V_{CM}. W praktyce napięcia V_{CM} ustawiane są automatycznie przez układ FPGA po programowym wyborze danego standardu, a wejściowe napięcia zmienne podawane są przez kondensatory separujące i obciążone rezystancjami 50 Ω do 100 Ω (rys.14), co upraszcza projektowanie takich układów i w praktyce zawsze daje dobre wyniki aplikacyjne.



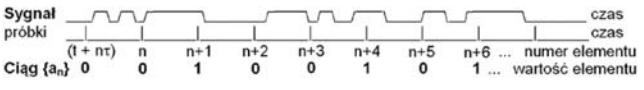
Rys.12. Zakresy zmienności napięć sygnałów w standardach CML, LVDS, LVPECL i VLM na tle napięć odniesienia V_{CM}

Kreacja binarnego ciągu losowego

Najważniejszym zagadnieniem dla dalszego przebiegu prac było odebranie przez transciver układu FPGA sygnału Poissona z rysunków 9 i 10 i próbkowanie jego wartości w celu otrzymania binarnego ciągu losowego. Ta pozornie trywialna operacja jest niezwykle ważna z dwóch powodów:

- próbkowanie sygnału Poissona wewnętrznym zegarem układu FPGA musi przypominać zwykłe „czytanie" jego chwilowych, binarnych wartości w trybie nieramkowym, bez żadnych dodatkowych operacji typu dekodowanie liniowe, kompensacja fazy, korekcja błędów FEC itp. [11],
- po próbkowaniu przechodzi się z dziedziny losowego sygnału w czasie rzeczywistym w dziedzinę losowego ciągu logicznego $\{a_n\}$ niemającego już związku z czasem, a jedynie organizację związaną z numeracją elementów ciągu; istotę tego przejścia ilustruje rysunek 13.
-

$$\{a_n\} = \begin{cases} 0 \text{ dla } X(t+n\tau) = -1 \\ 1 \text{ dla } X(t+n\tau) = +1 \end{cases}$$



Rys.13. Próbkowanie sygnału Poissona i kreacja ciągu losowego

Sygnał próbkowany z zegarem o częstotliwości f_P = 1 GHz daje oczywiście wynikowy ciąg binarny o zakładanej przepływności 1 Gbit/s. Nie należy jednak obawiać się, że dalsze operacje wewnątrz układu FPGA będą wykonywane z tak dużymi szybkościami, zresztą nieosiągalnymi w nawet zaawansowanych układach, które są w stanie przetwarzać sygnały logiczne z zegarami sięgającymi 600 MHz. Okazuje się, że transcivery układów FPGA są wspierane sprzętowo przez układy tzw. serializerów i deserializerów, tzn. układów przeorganizowujących strumienie równoległe na szeregowe i odwrotnie. Składają się one z układów rejestrowych o n-komórkach, gdzie n = 8÷80, z pośrednimi wartościami n = 16, 32, 64 i innymi. Stąd ciąg o przepływności 1 Gbit/s na wejściu takiego rejestru w dalszej obróbce ma organizację słów n-elementowych o przepływności 1 Gbit/s / n, tzn. dla n = 8 jest odpowiednio 125 MB/s, a dla n = 80 zaledwie 12,5 M(80 elementów)/s, co pozwala wykonywać dalsze operacje z zegarami odpowiednio 125 MHz oraz 12,5 MHz. W tak szybkim układzie FPGA, jak 5AGTMC7G3F31I3N, można zastosować oba te zegary i dowolny pośredni, a ich wybór jest kwestią koncepcji i projektu układu logicznego.

Analiza układu kreacji binarnego ciągu losowego

Badania tak wygenerowanych ciągów można prowadzić dwiema metodami – lokalną, wewnątrz układu FPGA, lub zdalną – w komputerze odbierającym ciągi z układu FPGA.

Analizując schemat z rysunku 5 należy jednak zauważyć, że każdy generator ciągów losowych musi mieć własne, wbudowane mechanizmy testowania i weryfikowania źródłowej losowości ciągów. Ponieważ wymagania te dotyczą źródłowej entropii, która jeśli nie spełnia wymagań, to powoduje generację ciągu nielosowego, którego nie ma sensu wysyłać do komputera, a jedynie informację alarmu o niezdolności do dalszej, poprawnej pracy. Wynika stąd, że jeśli układ FPGA będzie w stanie kontrolować, w sensie mierzyć entropię w czasie rzeczywistym, a jej wartość będzie się mieściła w zakresie wymaganym do uznania ciągu za doskonale losowy, to badania wygenerowanych ciągów przesłanych do komputera powinny mieć charakter kontrolny i w każdej próbie ciągu dawać wynik pozytywny.

Wymaga to dokładniejszej analizy tego schematu, aby przypisać przedstawionym na nim blokom funkcjonalnym i opisującym je pojęciom rzeczywiste odpowiedniki układowe i sygnałowe opisywanej koncepcji i konstrukcji generatora.

Analogue quantum noise source to klasycznie rozumiane, analogowe źródło losowego szumu. Nazwa nie nawiązuje więc wprost do wzmiankowanych, nanoskopowych zjawisk kwantowych w postaci superpozycji stanów kwantowych, czy rozpadu radioaktywnego, ale nawet rozszerza je na *optyczne* i *nieoptyczne* oraz *aktywne* i *pasywne*. Analizując istotę mikroplazmatycznego przebicia lawinowego złącza p-n można go również uznać za zjawisko kwantowe w skali mikroskopowej, ponieważ przejścia „paczek" elektronów przez barierę złącza są całkowicie przypadkowe w sensie nieprzewidywalności w kolejnej chwili czasu (*unpredictable*) i niepowtarzalności dowolnej realizacji w długim okresie czasu (*unrepeatable*). Układ mikrofalowego generatora sygnału Poissona można zatem uznać za kwantowe, nieoptyczne i aktywne źródło losowości, wpisujące się w te kryteria. Łatwo zauważyć, że takie same cechy i opis formalny, modelowany procesem Poissona, można też przypisać detekcji cząstek z rozpadu radioaktywnego, a sam opis odbiorowi pojedynczych fotonów oraz wielu innym zjawiskom w skali nanoskopowej [1]. Ważnym założeniem jest, że źródło losowości musi stanowić jeden zestaw wraz z układem pomiaru swego chwilowego stanu (*quantum state preparation* i *quantum state measurement*) [1], w tym przypadku rozumianym jako układ próbkowania aktualnego stanu w postaci chwilowej wartości sygnału Poissona.

Równolegle z nimi działa układ monitorowania źródła (*source parameter monitoring*), domyślnie układ weryfikacji entropii, jednak nie tyle źródła, które może być przecież analogowe, ile wyniku działania następującego po nim układu pomiarowego. Jeśli wynikiem tego działania jest losowy ciąg binarny, to oczywistym kryterium weryfikacji losowości źródła jest pomiar i kwalifikacja bieżącej entropii właśnie ciągu losowego, wygenerowanego ze źródłowego szumu. Ciąg ten musi zostać zapisany w buforze, jako że entropia jest właściwością ciągu zmiennych losowych, więc musi być badana i weryfikowana na podstawie próby ciągu o odpowiednio dużej liczebności. Odbywa się to w układzie akwizycji (*raw data acquisition*). Całość stanowi *digital quantum noise source*, czyli cyfrowe źródło ciągów (*raw data*) o entropii teoretycznie określonej *a priori* i na bieżąco weryfikowanej, tzn. technicznie mierzonej *a posteriori*.

Jeśli próba ciągu spełnia kryteria losowości w sensie zakładanej entropii (*entropy verification*), to ciąg jest oddawany na wyjście operacyjne (*entropy source output*) generatora ciągów losowych, opisanego jako *quantum entropy source*, a jeśli nie, to na jego wyjściu informacyjnym pojawia się komunikat o błędnym działaniu (*error message*).

Można jeszcze wspomnieć o bloku przetwarzania ciągów, zweryfikowanych wstępnie, jako losowe. Odbywa się to w opcjonalnym układzie *post-processing*. Niestety, w praktyce żaden pojedynczy generator ciągów losowych, wykonany zgodnie ze schematem z rysunku 5, nie spełnia nawet podstawowych wymagań, niezależnie od tego, czy wynikają one z kryptograficznych kryteriów opartych na entropii, czy kryteriów testów statystycznych. Wynika to stąd, że ani w przyrodzie, ani tym bardziej w technice nie ma źródeł o jednostkowej entropii, ponieważ musiałaby charakteryzować je nieskończenie duża szybkość działania, w przypadku sygnału Poissona z kryterium $\lambda \to \infty$. Stąd jako układy „poprawiające" entropię stosuje się różne algorytmiczne „ekstraktory entropii", sztucznie maskujące jej wartość, zasadniczo z intencją oszukania testów statystycznych. Najpopularniejszym „ekstraktorem", wspominanym również w dokumencie [5], jest haszująca funkcja skrótu. Jednak w kryptografii takie działania uznaje się za teoretycznie niedopuszczalne i prawnie zabronione. Wynika to stąd, że zgodnie z teorią informacji, entropia jest właściwością źródłową i nie można jej w żaden sposób powiększyć, natomiast większość fizycznych operacji na sygnałach, a nawet logicznych na ciągach może ją tylko zmniejszyć [12].

Nie oznacza to oczywiście, że mając generator ciągów losowych o niejednostkowej entropii, nie można wykonać generatora ciągów doskonale losowych o praktycznie jednostkowej entropii. Wymaga to jednak układu *post-processingu* nie w postaci algorytmicznego „ekstraktora entropii", a kilku generatorów, których ciągi wyjściowe będą poddane logicznej operacji XOR. I tylko w ten prosty, choć kosztowny sposób można osiągnąć w zbiorczym ciągu wynikowym praktycznie jednostkową entropię [2].

Koncepcja badania entropii binarnego ciągu losowego

Badania entropii wymagają uprzedniego zdefiniowania kilku pojęć, które wyraźnie oddzielają probabilistykę od statystyki. Takie pojęcia, jak prawdopodobieństwo i entropia są właściwościami ciągu zmiennych losowych, opisujących dany proces losowy *a priori* i jako takie są niemierzalne. Nas interesuje jednak pomiar właściwości i parametrów ciągów, jako realizacji procesu losowego *a posteriori*, czyli po zapisaniu próby ciągu o danej liczebności. Takie pojęcia nazywa się statystykami średniej z próby i entropii z próby.

Potrafiąc poprawnie modelować właściwości i parametry zmiennych losowych danego procesu losowego, można po zapisaniu próby ciągu, stanowiącego wynik realizacji tego procesu, porównać je i stwierdzić zgodność nie tylko właściwości, ale właśnie takich parametrów, jak entropia z próby i entropia *a priori*, czy średnia i prawdopodobieństwo.

W pierwszym etapie modelowania należy opisać ciąg losowy wygenerowany na podstawie próbkowania sygnału Poissona. Najprostszym, ale w pełni zgodnym modelem takiego ciągu jest łańcuch Markowa 1. rzędu, w którym zakłada się zależności tylko między sąsiednimi elementami [2]. Opisuje go zaledwie sześć prawdopodobieństw: $P(0) = 1/2 - s$, $P(1) = 1/2 + s$, $P(0,0) = 1/4 - s + 1/4\ K$, $P(0,1) = 1/4 - 1/4\ K$, $P(1,0) = 1/4 - 1/4\ K$ i $P(1,1) = 1/4 + s + 1/4\ K$, gdzie $s = P(0) - P(1)$, to różnica między prawdopodobieństwami występowania zer i jedynek, a $K = P(0,0) + P(1,1) - P(0,1) - P(1,0)$, to w praktyce zawsze dodatni współczynnik korelacji między sąsiednimi elementami łańcucha (x_n, x_{n+1}).

Entropia tak zdefiniowanego ciągu dla najważniejszej w modelu łańcucha Markowa zmiennej losowej (X_1, X_2) dana jest jako $H(X_1, X_2) = -\sum_{i,j} P(X_i, X_j) \log_2 P(X_i, X_j) \approx 1 - \{ (2s)^2 + 1/2\ K^2 \} / 2\ln 2$, a niedokładność takiego przybliżenia względem zależności Shannona wynosi około $2s^4 + (2K)^4$.

Taką samą zależnością dana jest entropia z próby N-elementowej i wyznaczonymi pomiarowo $s = (n_0 - n_1) / N$, gdzie $n_0 + n_1 = N$ oraz $K = (n_{0,0} + n_{1,1} - n_{0,1} - n_{1,0}) / N/2$.

Wartość s w przypadku sygnału Poissona wynika głównie z niestabilności jego wartości średniej, dającej niewielką i zmienną nierównowagę zer i jedynek w każdej próbie ciągu.

Wartość K pochodzi z właściwości korelacyjnych tego sygnału i dana jest jako $K = \exp(-2\lambda / f_P)$, gdzie λ jest jego gęstością zmian, a f_P jest częstotliwością próbkowania.

Jak zatem widać, jest to prosty model teoretyczny, łatwo weryfikowalny pomiarowo. Okazuje się jednak, że model ten można jeszcze bardziej uprościć w sensie implementacji pomiarowej. Mało znaną właściwością ciągów losowych jest ta, że średnia liczba zmian z zer na jedynki wynosi 1/4 liczebności próby ciągu [13]. Jeśli ciąg jest zorganizowany czasowo jako strumień danych o przepływności BR, to mierząc częstość występujących w nim zmian otrzyma się wartość $f = BR / 4$. Tak jest jednak tylko w przypadku ciągu doskonale losowego, tzn. dla $s = K = 0$. Jeśli te wartości nie są zerowe, to otrzyma się $f = BR / 4\ (1 - (2s)^2 - K)$, a ponieważ dla np. $s < 0{,}01$ i $K < 0{,}05$ można przy $K < 0{,}05$ zaniedbać składnik $(2s)^2 < 0{,}0004$, więc $f \approx BR / 4\ (1 - K)$. Pomiar nierównowagi zer i jedynek oraz częstotliwości zmian z zer i jedynki jest w układach programowalnych FPGA prosty realizacyjnie i pozwala łatwo mierzyć w czasie rzeczywistym wartość entropii danej jako $H(X_1,X_2) = 1 - \{ (2s)^2 + 1/2\ K^2 \} / 2\ln 2$, a przy obniżeniu jej wartości poniżej przyjętego kryterium wszczynać alarm o nielosowości. Taka koncepcja pomiaru entropii ma jeszcze jedną zaletę – układ akwizycji (*raw data acquisition*) nie musi posiadać pamięci na rejestrację długich prób ciągów do obliczeń *off line*, ponieważ pomiar nierównowagi s oraz częstotliwości zmian f i wynikających z nich korelacji K odbywa się *on line* i w dowolnym momencie, kiedy wartości te przekroczą założone kryteria, układ weryfikacji entropii (*entropy verification*), wyłączy wyjście operacyjne (*entropy source output*) a na wyjście informacyjnym wyśle komunikat o błędnym działaniu (*error message*). Ponadto, zgodnie z zaleceniami z dokumentu [5] wyjście informacyjne może również służyć do ciągłego monitoringu entropii, której wartości $H(X_1, X_2)$ wraz z wartościami s i K mogą być na bieżąco wysyłane, monitorowane i archiwizowane w odbiorniku ciągów losowych, zwykle właśnie komputerze.

Wracając do pojęcia badania źródłowej entropii można zadać pytanie, czy nie należałoby jednak badać losowości sygnału Poissona w sensie źródłowego pomiaru gęstości zmian λ i wyznaczaniu na jego podstawie wartości funkcji autokorelacji $K = \exp(-2\lambda / f_P)$? Niestety, jest to niemożliwe, ponieważ sygnał Poissona wprowadzony na wejścia odbiornika transceivera musi być od razu próbkowany i nie

jest możliwe wprowadzenie jego źródłowej, asynchronicznej postaci do wnętrza układu programowalnego FPGA. Gdyby nawet było to jednak możliwe, to sygnał, którego chwilowa gęstości zmian λ sięga kilku GHz, nie mógłby być przetwarzany w sensie np. licznikowym, skoro maksymalne częstotliwości przerzutników w takich układach sięgają 600 MHz. Można dodać, że praca z takimi częstotliwościami też jest praktycznie niemożliwa, stąd właśnie koncepcje przejść od organizacji szeregowej do równoległej i przetwarzanie nawet 100 Git/s strumieni danych w postaci równoległej z typowymi zegarami nieprzekraczającymi 150 MHz.

Technika badania entropii binarnego ciągu losowego

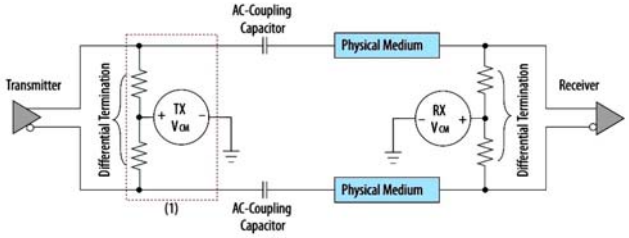
Na etapie badań wstępnych można nie badać wynikowej wartości entropii ciągów, tylko wartości s i K, od których ona zależy. Wynika to stąd, na potencjalne obniżanie entropii $H(X_1, X_2) = 1 – \{ (2s)^2 + 1/2\ K^2 \} / 2\ln 2$ obie te wartości mają praktycznie ten sam wpływ w sensie wartości $(2s)^2$ i $1/2\ K^2$. Chcąc zatem poprawić sprzętowo działanie układu w sensie zwiększenia entropii, należy wiedzieć, który ma jaki wpływ, by każdy z nich doprowadzić do jak najniższego poziomu, najlepiej $(2s)^2 \approx 1/2\ K^2$.

W praktyce, o ile minimalizacja wartości s jest dość prosta sprzętowo, o tyle wartość K zależy od właściwości i parametru gęstości zmian λ sygnału Poissona, co można korygować, w sensie zmniejszać K przez zwiększanie λ, zmieniając źródłową diodę lawinową na szybszą. Nie jest to jednak takie proste, ponieważ wymaga dopasowania takiej diody w układzie z rysunku 6, ewentualnych modyfikacji układowych w sensie wymiany i dopasowania wzmacniaczy MMIC, zapewnienia wynikowej stabilności całego układu, poziomu napięć wyjściowych – wszystko w odpowiednio szerszym paśmie mikrofalowym. Nie należy też zapominać, że na wartość współczynnika korelacji K ma wpływ nie tylko gęstości zmian λ, ale wiele innych, pobocznych czynników, zwłaszcza zakłóceń, które mogą zmienić nie tylko jego wartość, ale nawet znak. Jeśli ta wartość będzie niewielka, ale o znaku ujemnym, to nie należy cieszyć się z entropii o podwyższonej wartości, wynikającej z czynnika $(–K_X)^2 < K_P^2$, ponieważ taki sygnał nie jest Poissona, a wynikowy ciąg nie odpowiada modelowi łańcucha Markowa 1. rzędu. Można tylko wspomnieć, że wykorzystując miarę $f = BR / 4\ (1 – K)$ również można wykrywać takie anomalie, ponieważ dla $K < 0$ otrzymany $f = BR / 4\ (1 – (– K) = BR / 4\ (1 + K) > BR / 4$. Z praktyki wynika też, że ciąg wygenerowany na podstawie takiego sygnału może „wyglądać jak losowy” (*looks like random*) i nawet spełniać wybrane testy statystyczne, ale przy dokładniejszych badaniach okaże się nielosowy, bo jego statystyki będą w większej mierze pochodnymi właśnie zakłóceń, niż źródłowego sygnału Poissona.

Z powyższych względów, mówiąc o badaniu i pomiarach entropii, lepiej jest widzieć ją jako wartość zmniejszaną przez oba czynniki, tzn. $(2s)^2$ i $1/2\ K^2$ i wymagać, aby każdy z nich miał odpowiednio małą wartość, np. $(2s)^2 \approx 1/2\ K^2 < 0{,}0004$, a stąd $s < 0{,}01$ i $K < 0{,}03$. Może to mieć również znaczenie techniczne w sensie serwisowania – wartość s zależy zasadniczo od różnych czynników i ograniczeń sprzętowych, ale jest praktycznie stała w czasie. Natomiast wartość K zależy od gęstości zmian λ sygnału Poissona z diody lawinowej, która w czasie pracy stopniowo „wypala” się, co zawsze powoduje zmniejszanie się wartości λ, aż do momentu, kiedy wynikowa wartość K przekroczy np. $K > 0{,}03$, co spowoduje zmniejszenie się entropii ciągu poniżej wartości $H < 0{,}9994$, spełniając kryterium wysłania komunikatu o błędnym działaniu (*error message*). Taka zmiana nie następuje skokowo, ale jest wynikiem dłuższej eksploatacji, stąd bieżąca kontrola w sensie wysyłania, monitorowania, archiwizowania i analizy takich parametrów w odbiorniku ciągów losowych ma głęboki sens.

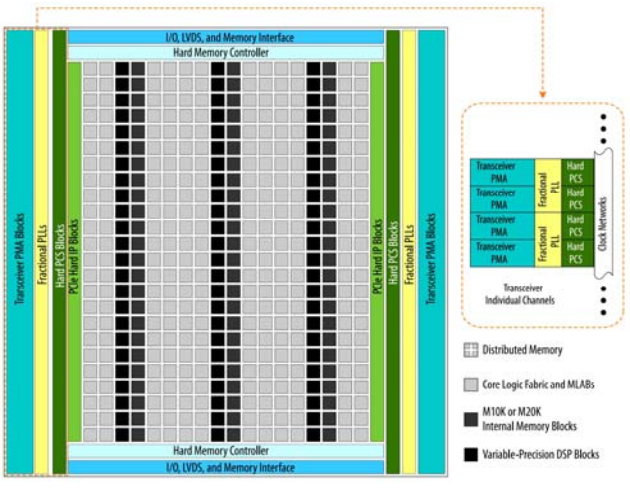
Układ do badania entropii binarnego ciągu losowego

W dalszym ciągu przedstawiono koncepcję pomiarów wartości s i K przez układ 5AGTMC7G3F31I3N z rysunku 11 (*receiver*) z dołączonymi poprzez 50 Ω symetryczną linię transmisyjną w postaci ekranowanej skrętki (*physical medium*) układami mikrofalowych generatorów sygnału Poissona (*transmitter*) z rysunku 6. Użyto do tego ekranowanej skrętki USB 3.0 (SS), przenoszącej sygnały cyfrowe do 5 Gbit/s, ponieważ wejścia transceiverów układu FPGA są dopasowane do takich połączeń – rysunek 14.



Rys.14.Połączenie układu 5AGTMC7G3F31I3N z układem mikrofalowego generatora sygnału Poissona [11]

Wewnętrzną strukturę układu 5AGTMC7G3F31I3N oraz części składowe transceiverów przedstawia rysunek 15 [11]. Składają się one z dwóch warstw. Pierwszej – PMA (*physical medium attachment*), odpowiedzialnej za fizyczny odbiór i zmianę organizacji danych strumienia szeregowego do postaci równoległej. Drugiej – PCS (*physical coding sublayer*), odpowiedzialnej za logiczne połączenie buforów z danymi w postaci równoległej z rdzeniem (*core*) układu FPGA. Układy PMA, zgodnie z założeniem o próbkowaniu sygnału Poissona, zostały skonfigurowane do pracy nieramkowej *PMA direct*. Okazuje się, że w tym trybie pracy warstwa PCS jest omijana (*by-pass*) i dane z buforów PMA mogą być wprowadzane bezpośrednio do rdzenia FPGA. PMA i PCS mogą pracować z zegarem o maksymalnej częstotliwości 160 MHz, co dla buforów 8-bitowych pozwala na transfer do 1,3 Gbit/s, ale dla 80-bitowych aż 13 Gbit/s. Okazuje się, że w trybie *PMA direct* możliwa jest praca z zegarem próbkującym o częstotliwości do 10,315 GHz i buforami 8-, 10-,16-, 20-, 32-, 40-, 64- i 80-bitowymi, z tym, że zalecany jest ten ostatni i ustawiony jest jako domyślny. Przy zegarze 10,315 GHz pozwala to operować słowami 80-bitowymi z zegarem 129 MHz, mniejszym od 160 MHz. Należy jednak pamiętać, że takie wybory i szacowania muszą zostać potwierdzone poprawnymi projektami, dla układów 5AGTMC7G3F31I3N wykonanymi w projektowym, programistycznym środowisku *Intel Quartus Prime Pro* [11].



Rys.15.Wewnętrzna struktura układu 5AGTMC7G3F31I3N i części składowe jego transceiverów [11]

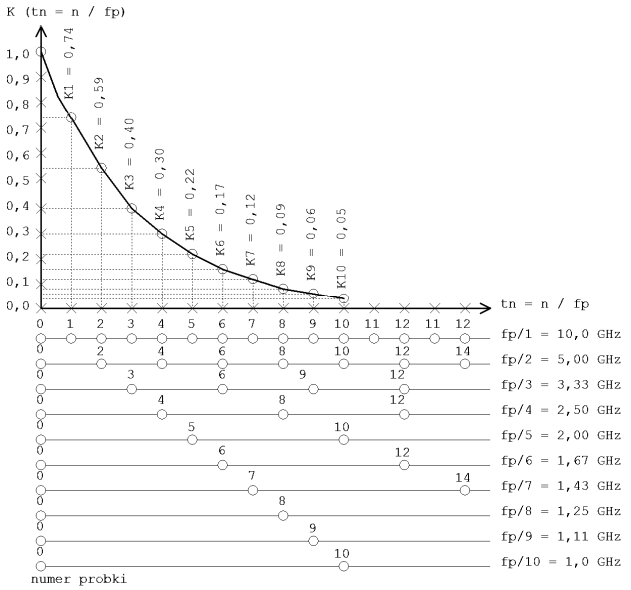
Wyniki badania entropii binarnego ciągu losowego

Przed rozpoczęciem pomiarów należy jeszcze dokonać wyboru częstotliwości zegara układu próbkującego. Zegar ten dla układu 5AGTMC7G3F31I3N może mieć od 600 MHz do 10 GHz. Intencją niniejszej pracy jest analiza możliwości generacji ciągów losowych z przepływnością 1 Gbit/s, więc naturalnym byłaby wybór wartości 1 GHz. Użycie częstotliwości 10 GHz nic jednak nie kosztuje, a może dać interesujące odpowiedzi na dwa istotne pytania:

- jaka jest maksymalna częstotliwość próbkowania danego sygnału Poissona, przy której wartości s i K mają jeszcze dopuszczalnie małe wartości; gdyby ta częstotliwość była większa od 1 GHz, to można by mówić o generatorze ciągów losowych o przepływności większej, niż 1 Gbit/s,
- jak wygląda nie pojedynczy współczynnik korelacji K, ale cała funkcja autokorelacji $K(t_n)$, mierzona punktowo dla wybranych przedziałów czasu $t_n = n / f_P$; wyznaczenie takiej funkcji umożliwiłoby weryfikację modelu sygnału Poissona w sensie pośredniego sprawdzenia jego funkcji widmowej gęstości mocy $G(\omega)$, a nawet gęstości zmian λ.

Próbkując w ten sposób sygnał Poissona, dane są wyniki próbkowania z częstotliwościami 10 GHz, 5 GHz, 3,33 GHz, 2,5 GHz, 1,67 GHz, 1,43 GHz, 1,25 GHz, 1,11 GHz i 1 GHz.

Próbki te uzyskuje się, pobierając wszystkie próbki dla 10 GHz, co drugą próbkę dla 5 GHz, co trzecią dla 3,33 GHz i kolejno, do co dziesiątej próbki dla 1 GHz. Sposób wyboru próbek i wyznaczenia funkcji autokorelacji $K(t_n = n / f_P)$ na podstawie danych z tabeli 1 ilustruje rysunek 16.



Rys.16. Sposób wyboru próbek i wyznaczenia funkcji autokorelacji $K(t = n / f_P)$

W tabeli 1 przedstawiono wyniki pomiarów wartości s_n i K_n oraz obliczonych entropii $H(s_n, K_n)$ i gęstości zmian λ_n dla danej częstotliwości próbkowania f_P = 10 GHz / n. Wszystkie otrzymane wartości są wzajemnie spójne, czym w ogólności potwierdzają poprawność założeń i wyników analiz całego procesu generacji, w szczególności zgodność modelu rzeczywistego sygnału Poissona. Wartości entropii można uznać za wysokie, ale jednak niższe niż pożądane 0,9999. Miały na nie wpływ oba składniki, $(2s)^2$ i 1/2 K^2, co wymaga spójnych pomiarów w procesie weryfikacji entropii.

Z wyników badań przedstawionych w tabeli 1 wypływają następujące wnioski:

- źródłowy sygnał Poissona i wynikowy łańcuch Markowa 1. rzędu są uniwersalnymi modelami, umożliwiającymi prosty i spójny, sygnałowy i probabilistyczny opis wszystkich faz procesu generacji ciągów losowych oraz pomiary entropii, zgodnie ze schematem z rysunku 5,
- konstrukcja mikrofalowego generatora sygnału Poissona oraz technologie użyte do jego przetwarzania w układach FPGA zostały dobrze opanowane, zaimplementowane technicznie i poprawnie zamodelowane matematycznie,
- mikrofalowy sygnał Poissona o gęstości zmian co najmniej λ **= 1,5 GHz mo·e by· ·r d·em do kreacji binarnego ci·gu losowego o przep·ywno·ci 1 Gbit/s,**
- **zweryfikowana pomiarowo entropia takiego ci·gu jest wi·ksza od** $H(X_1, X_2) > 0{,}998$ bit/element,
- na osiągalnie niejednostkowej entropii ciągu współmierny wpływ mają nierównowaga zer i jedynek s, wynikająca z niestabilności wartości średniej sygnału Poissona oraz korelacje międzyelementowe, opisane współczynnikiem korelacji K, wynikającym ze skończonej gęstości zmian λ,
- otrzymany ciąg nie ma idealnych parametrów w sensie niejednostkowej entropii, ale potwierdzone pomiarowo właściwości modelu łańcucha Markowa 1. rzędu, można zatem postawić tezę, że jest tworzywem do uzyskania doskonale losowego ciągu o jednostkowej entropii.

Tab.1. Wyniki pomiarów w funkcji częstotliwości próbkowania f_{P_n}

f_{P_10}	s_{10}	K_{10}	$H(s_{10}, K_{10})$	λ_{10}
10 GHz / 10 = 1,0 GHz	0,015	0,05	0,998	$1{,}5\ 10^9$
f_{P_9}	s_9	K_9	$H(s_9, K_9)$	λ_9
10 GHz / 9 = 1,11 GHz	0,015	0,06	0,998	$1{,}5\ 10^9$
f_{P_8}	s_8	K_8	$H(s_8, K_8)$	λ_8
10 GHz / 8 = 1,25 GHz	0,015	0,09	0,996	$1{,}5\ 10^9$
f_{P_7}	s_7	K_7	$H(s_7, K_7)$	λ_7
10 GHz / 7 = 1,43 GHz	0,015	0,12	0,994	$1{,}5\ 10^9$
f_{P_6}	S_6	K_6	$H(s_6, K_6)$	λ_6
10 GHz / 6 = 1,67 GHz	0,015	0,17	-	$1{,}5\ 10^9$
f_{P_5}	s_5	K_5	$H(s_5, K_5)$	λ_5
10 GHz / 5 = 2,00 GHz	0,015	0,22	-	$1{,}5\ 10^9$
f_{P_4}	s_4	K_4	$H(s_4, K_4)$	λ_4
10 GHz / 4 = 2,50 GHz	0,015	0,30	-	$1{,}5\ 10^9$
f_{P_3}	s_3	K_3	$H(s_3, K_3)$	λ_3
10 GHz / 3 = 3,33 GHz	0,015	0,40	-	$1{,}5\ 10^9$
f_{P_2}	s_2	K_2	$H(s_2, K_2)$	λ_2
10 GHz / 2 = 5,00 GHz	0,015	0,55	-	$1{,}5\ 10^9$
f_{P_1}	s_1	K_1	$H(s_1, K_1)$	λ_1
10 GHz / 1 = 10,0 GHz	0,015	0,74	-	$1{,}5\ 10^9$

Uwaga: obliczenia entropii dla K > 0,15 są niedokładne (zawyżone)

Podsumowanie

Przedstawiona analiza, symulacje układowe i wyniki eksperymentów stanowią kolejne podejście autorów do elektronicznych aplikacji mikrofalowych, ale pierwsze w sensie operowania na sygnałach losowych. Nie różni się ono jednak istotnie od np. aplikacji układów w standardach Ethernet 1000Base-FX, a nawet 10GBase-FX. Osiąganie poprawnych wyników w tej dziedzinie w każdym przypadku wymaga jednak ścisłego zachowania zasad pracy układów mikrofalowych i wykorzystania standardowych, modułowych komponentów, pozwalających na proste, łatwe i skuteczne składanie docelowych układów z wcześniej sprawdzonych bloków funkcjonalnych. Teza, że *wszystko powinno być tak proste, jak to tylko możliwe, ale nie prostsze*, sprowadza się w przypadku tego problemu do głębszej analizy sygnałów stochastycznych oraz zastosowania dość zaawansowanych technologii. W przypadku nietypowego problemu należy jednak zakładać wyjście poza znane i typowe rozwiązania.

Analizy i eksperymenty zostały zakończone na etapie uzyskania źródłowego ciągu o entropii 0,998 bitu na element ciągu. W kolejnej pracy zostanie opisana techniczna metoda osiągania praktycznie jednostkowych

entropii takich ciągów i matematyczny dowód ich warunkowego bezpieczeństwa kryptograficznego.

***Autorzy**: dr hab. inż. Marek Leśniewicz, profesor WIŁ-PIB, mgr inż. Piotr Komorowski, Janusz Zabłocki, Zakład Kryptologii WIŁ-PIB, 05-130 Zegrze, Warszawska 22A, E-mail: m.lesniewicz@wil.waw.pl*

LITERATURA

[1] Herrero-Collantes M., Garcia-Escartin J.C., Quantum random number generators, *Reviews of Modern Physics*, 2017, nr 1.
[2] Leśniewicz M., Sprzętowa generacja losowych ciągów binarnych, *Wydawnictwo Wojskowej Akademii Technicznej*, 2009.
[3] Leśniewicz M., Komorowski P., Metoda i układ powielania ciągów losowych, *Przegląd Elektrotechniczny*, 2021, nr 8.
[4] Réfrégier P., Noise Theory and Application to Physics – From Fluctuations to Information, *Springer Science*, 2004.
[5] Recommendation X.1702, Quantum noise random number generator architecture, *ITU-T*, 11/2019.
[6] Johnston D., Random Number Generators – Principles and Practices, *Walter de Gruyter Press*, 2018.
[7] Kollmitzer C., Schauer S., Rass S., Rainer B., Quantum random number generation, *Springer Nature*, 2020.
[8] Noise Products, www.noisecom.com, www.noisewave.com
[9] Steer M., Microwave and RF Design, vol.1-5, *NC SU*, 2019.
[10] ERA-1+ Monolithic InGaP HBT MMIC Amplifier, *Mini-Circuits.*
[11] Arria V Device Handbook, Volume 1: Device Interfaces and Integration, Volume 2: Transceivers, *INTEL (ALTERA)*, 2020.
[12] Seidler J., Nauka o informacji, *WNT*, 1983.
[13] Leśniewicz M., Patent nr 228827 pt. Sposób wykrywania utraty synchronizacji kryptograficznej i jej odzyskiwania, *UPRP*, 2015.