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

Raport z realizacji badań przemysłowych w ramach etapu nr 2 projektu, pt. "JURAND - Narodowy Kwantowy Generator Liczb Losowych"

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

Przedmiotem realizacji etapu nr 2 projektu ”JURAND - Narodowy Kwantowy Generator Liczb Losowych” były badania procesów kwantowych dla celów generacji liczb losowych w zakresie charakterystyki ich dynamiki kwantowej i niedeterminizmu mechanizmów fizycznych w reżimie praw mechaniki kwantowej celem wyboru najoptymalniejszych i najefektywniejszych z nich do wykorzystania w prototypowaniu kwantowego generatora liczb prawdziwie losowych.

Problematyka wyboru najbardziej optymalnych procesów kwantowych do realizowanych w etapie nr 3 projektu dalszych prac prototypowych nad praktycznym krajowym kwantowym generatorem liczb losowych jest wielopłaszczyznowa i obejmuje zarówno aspekty trudności implementacyjnej samych procesów kwantowych, tak aby realizowały one zadaną dynamikę możliwie bliską teorii (tj. minimalizując odchylenia implementacyjne od kwantowego niedeterminizmu), a także aby układy te pozostawały możliwe proste w zakresie konstrukcyjnym dla ich optymalizacji miniaturyzacyjnej i kosztowej w kierunku uzyskania zintegrowanych komponentów przy jednoczesnym zapewnieniu praktycznych poziomów parametrów technicznych szybkości generacji binarnych ciągów losowych i niezawodności.

W ramach etapu nr 2 zgodnie z harmonogramem projektu prowadzone były badania, które dotyczyły pięciu potencjalnych procesów kwantowych jako właściwych dla generacji liczb prawdziwie losowych:

- Kwantowego szumu śrutowego (komponenta szumu elektronowego pochodząca od kwantowego zjawiska tunelowania elektronów w nanoskopowo integrowanych układach elektronicznych MOS/CMOS)
- Efektu foto-elektrycznego (w zakresie oddziaływania światła i materii w opisie złotej reguły Fermiego, tj. kwantowej emisji fotonowej wraz z detekcją pojedynczo-fotonową za pośrednictwem detektorów w postaci diód lawinowych lub fotopowielaczy), w tym także z ewentualnym uwzględnieniem:

- Efektów szumowych w ramach kwantowej nano-plazmoniki w domieszkowanych metalicznie półprzewodnikach (pośrednictwo plazmonów w efekcie PV jako kwantowy stopień swobody o silnie emisyjnym charakterze w bliskim i dalekim polu modelowanym przez radiacyjne tarcie Lorentza i sprzężenia plazmonów z elektronami pasmowymi z uwzględnieniem poprawek wynikających z efektów czysto kwantowych)
- Optyki kwantowej (w tym efektów dwójłomności i polaryzacji światła w szczególności w zakresie polaryzacyjnych rozdzielaczy wiązki jak również efektu splątania kwantowego polaryzacji fotonów przy przejściu przez silnie dwójłomny nieliniowy kryształ beta boranu baru BBO w ramach procesu spontanicznej parametrycznej konwersji w dół SPDC)
- Procesów rozpadu jądrowego o małej promieniotwórczości (promieniowanie tła lub nisko-promieniotwórcze próbki np. soli potasu o naturalnej bezpiecznej radiacji, emitujące promieniowanie jonizujące jako źródło szumu kwantowego).

Rezultaty merytoryczne przeprowadzonych badań opublikowane zostały w szeregu specjalistycznych publikacji technicznych, w tym na platformie komercjalizacji kryptografii kwantowej (tzw. kwantowej dystrybucji klucza QKD), prowadzonej od 2005 roku przez realizatora projektu, tj. spółkę spin-off powołaną przez ekspertów dziedzinowych w celu komercjalizacji tej technologii, warunkowanej przez jej krytyczne komponenty w postaci kwantowych generatorów liczb prawdziwie losowych (QRNG).

Rezultaty merytoryczne prac badawczych przeprowadzonych w toku etapu nr 2 (wraz z cząstkowymi rezultatami prowadzonych prac etapu nr 3) obejmują następujące pozycje (przy numeracji kontynuującej zakres merytoryczny wyników z poprzedniego raportu z realizacji etapu nr 1 projektu):

- R-2: Raport z realizacji badań przemysłowych w ramach etapu nr 2 projektu, pt. ”JURAND - Narodowy Kwantowy Generator Liczb Losowych”, kamień milowy z realizacji etapu 2 projektu – niniejszy dokument
- P-4: Publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Analiza źródeł entropii dla kwantowej losowości”, w ramach której omówione są wyniki prac badawczych w zakresie efektów kwantowych mogących być źródłem generacji sekwencji losowych celem określenia najbardziej optymalnych źródeł dla empirycznych badań laboratoryjnych charakterystyk źródeł losowości https://seqre.net/sites/default/files/resources/generic/jurand/P-4-analiza-qrng.pdf
- P-5: Publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Wizualizacja wyników badań empirycznych procesów kwantowych określonych w wyniku badań przemysłowych jako najoptymalniejsze dla generacji liczb prawdziwie losowych, na podstawie przykładowych próbek losowych ciągów binarnych wygenerowanych laboratoryjnie w ramach ww. procesów kwantowych” https://seqre.net/sites/default/files/resources/generic/jurand/P-5-wizualizacja-empiryczna.pdf

- P-6: Publikacja w języku angielskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. ”Beam splitter and polarization beam splitter quantitative testing” https://seqre.net/sites/default/files/resources/generic/jurand/P-6-measurements.pdf
- P-7: Publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Weryfikacja nieklasycznego rezultatu złamania nierówności Bella dla stanow splątanych (złamanie limitow statystyki klasycznej w korelacjach splątaniowych) jako fundamentalny test kwantowej losowości” https://seqre.net/sites/default/files/resources/generic/jurand/P-7-zlamanie-nierownosci-bella.pdf
- P-8: Publikacja w języku angielskim w międzynarodowym naukowym czasopiśmie dziedzinowym Scientific Reports wydawnictwa Nature Springer, pt. „Quantum random number generators with entanglement for public randomness testing”, 13 styczeń 2020 r., Scientific Reports, Nature Springer – https://www.nature.com/articles/s41598-019-56706-2 (p8-sci-rep-2020-qeqrng.pdf); publikacja uzykała 5-te miejsce w kolekcji 'Top 100 in Physics' w 2020 roku w czasopiśmie Scientific Reports (Nature Springer) [https://www.nature.com/collections/ihggebhehd]; IF 4.379, wykaz czasopism MEiN z dnia 9.02.2021r. lp. 18271, 140 pkt; https://seqre.net/sites/default/files/resources/generic/jurand/P-8-sci-rep-2020-qeqrng.pdf
- P-9: Publikacja w języku angielskim w międzynarodowym naukowym czasopiśmie dziedzinowym Scientific Reports wydawnictwa Nature Springer, pt. „Quantum generators of random numbers” wraz z informacjami dodatkowymi (Supplementary Information), 9 sierpnia 2021 r., Scientific Reports, Nature Springer – https://www.nature.com/articles/s41598-021-95388-7 (p9-sci-rep-2021-qrngSI.pdf i p9-sci-rep-2021-qrng-corrected-nobib.pdf), przedstawiająca także cząstkowe wyniki etapu nr 3 projektu w zakresie prototypowania układu QRNG; IF 4.379, wykaz czasopism MEiN z dnia 9.02.2021r. lp. 18271, 140 pkt; https://seqre.net/sites/default/files/resources/generic/jurand/P-9-sci-rep-2021-qrng.pdf; https://seqre.net/sites/default/files/resources/generic/jurand/P-9-sci-rep-2021-qrngSI.pdf
- P-10: publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „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” , przedstawiająca także cząstkowe wyniki etapu nr 3 projektu w zakresie prototypowania układu QRNG https://seqre.net/sites/default/files/resources/generic/jurand/P-10-ekspertyza-uzupelniajaca.pdf
- P-11: publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Układ akwizycji danych dla kwantowych generatorów liczb

losowych", przedstawiająca także cząstkowe wyniki etapu nr 3 projektu w zakresie prototypowania układu QRNG https://seqre.net/sites/default/files/resources/generic/jurand/P-11-uklad-akwizycji.pdf

- P-12: publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Zastosowanie pułapki optycznej do generatora liczb losowych" , przedstawiająca także cząstkowe wyniki etapu nr 3 projektu w zakresie prototypowania układu QRNG https://seqre.net/sites/default/files/resources/generic/jurand/P-12-pulapka-optyczna-poster.pdf
- P-13: publikacja w języku angielskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Random Quantum Noise Generation Using Shot Noise in Semiconductors", przedstawiająca także cząstkowe wyniki etapu nr 3 projektu w zakresie prototypowania układu QRNG https://seqre.net/sites/default/files/resources/generic/jurand/P-13-shot-noise-en.pdf
- P-14: publikacja w języku polskim na platformie internetowej komercjalizacji kryptografii kwantowej seQre.net, pt. „Kryptograficzna generacja liczb losowych wykorzystując szum śrutowy", przedstawiająca także cząstkowe wyniki etapu nr 3 projektu w zakresie prototypowania układu QRNG https://seqre.net/sites/default/files/resources/generic/jurand/P-14-shot-noise-pl-poster.pdf
- P-15: pozostająca w pośrednim związku z badaniami projektowymi publikacja w języku angielskim w postaci monografii „Quantum Nano-Plasmonics" wydanej w 2020 r. przez Cambridge University Press, w której członek zespołu badawczego projektu (W. A. Jacak) analizuje efekty kwantowe w nano-plazmonice w oryginalnie rozwiniętej teorii RPA w nano-cząstkach, których skala jednak w stosunku do energii dynamiki plazmonów okazuje się na tyle niewielka (np. efektu spill-out, tj. kwantowego wylewania się cieczy elektronowej poza cząstkę), że minimalizuje możliwości ich praktycznego wykorzystania do generacji losowości w pojedynczych plazmonowych nanoczastkach; pomimo, że w zintegrowanych układach potencjalnie opartych na domieszkowanych metalicznie nano-cząstkami diodach półprzewodnikowych wykazujących silne plazmonowe wzmocnienie zjawiska fotoelektrycznego w absorpcji fotonów padających na półprzewodnik sytuacja jest bardziej korzystna (ten plazmonowy efekt jest kwantowy i łatwo mierzalny), to jednak uwarunkowania tego procesu nie pozwalają na implementację praktycznego źródła generacji liczb losowych (największym problemem jest tu wzbudzanie plazmonu w nanocząstce w sposób kwantowy, gdyż energia plazmonu, tj. kolektywnego drgania cieczy elektronowej nie odpowiada skali energetycznej pojedynczych fotonów padających na plazmonicznie modyfikowaną fotodiodę, będących uwarunkowaniem kwantowej losowości źródła modelowanej statystyką według rozkładu Poissona) – z tego też powodu mechanizm fizyczny nano-plazmonicznego wzmocnienia efektu fotoelektrycznego dla generacji losowości kwantowej nie został określony jako najoptymalniejszy dla wykorzystania w generatorze

QRNG (mimo, że efekty kwantowe sprzężenia plazmonów z pasmowymi elektronami są dominujące i realizowane wg. złotej reguły Fermiego, a z uwagi na łatwość pomiarowa fotowoltaicznych efektów zjawiska takie mogłyby być traktowane jako perspektywiczne potencjalne źródła entropii dla QRNG wykorzystujące niedeterminizm kwantowy przejść według złotej reguły Fermiego) – zagadnienia te są szczegółowo i oryginalnie rozwinięte w monografii – sierpień 2020 r.
https://www.cambridge.org/core/books/quantum-nanoplasmonics/C1F1E45450A75B0B48520FFC5C6B365E;
https://seqre.net/sites/default/files/resources/generic/jurand/P-15-QuantumNano-Plasmonics_CambridgeUP_2020.zip

- P-16: (poster; zasięg międzynarodowy) J. E. Jacak, W. A. Jacak, W. A. Donderowicz, P. Jóźwiak, L. Jacak, Quantum random number generators with entanglement for public randomness testing, QCrypt 2020 (konferencja QCrypt 2020, 10-14 sierpień 2020, konferencja online)
https://seqre.net/sites/default/files/resources/generic/jurand/P-16-QCrypt2020-poster.pdf
- P-17: (poster; zasięg międzynarodowy) W. A. Jacak, J. E. Jacak, W. A. Donderowicz, P. Jóźwiak, L. Jacak, Multiqubit entanglement for public randomness testing vs Google's quantum supremacy, Quantum 2020 IOP, 2020 (konferencja Quantum2020 IOP Conference, 19-22 październik 2020, konferencja online)
https://seqre.net/sites/default/files/resources/generic/jurand/P-17-Quantum2020IOP-poster.pdf
- W-2: Dane empiryczne w postaci ciągów binarnych laboratoryjnie wygenerowanych w ramach procesów kwantowych określonych w wyniku badań przemysłowych jako najoptymalniejsze dla generacji liczb prawdziwie losowych (szumy śrutowe w układach elektronicznych oraz układy optyki kwantowej)
https://seqre.net/sites/default/files/resources/generic/jurand/W-2-dane-empiryczne.zip
- W-3: Dane źródłowe i statystyczne w zakresie prowadzonych analiz weryfikacji złamania nierówności Bella dla wykazania kwantowości procesu fizycznego źródła na podstawie korelacji splątaniowych
https://seqre.net/sites/default/files/resources/generic/jurand/W-3-wyniki-korelacji-bella.zip

W wyniku przeprowadzonych badań przemysłowych, których szczegółowe wyniki przedstawiają ww. pozycje raportowe, potwierdzono, że szum śrutowy w zintegrowanych układach elektronicznych, jako kwantowo-mechaniczna komponenta ogólnego szumu elektronowego możliwa do analizy w zakresie metod kwantowania dynamiki elektronów w układach scalonych jest najoptymalniejszym procesem dla realizacji wysoce zintegrowanych i zminiaturyzowanych a zarazem praktycznych i szybkich układów kwantowych generatorów losowości.

Zasada nieoznaczoności Heisenberga wyklucza możliwość jednoczesnego określenia położenia i prędkości poszczególnych cząstek kwantowych (np. elektronów), co wiąże się z ich fundamentalnym

kwantowo-mechanicznym niedeterminizmem. W zakresie tej teorii (zweryfikowanej empirycznie i wykazanej jako obowiązującej w skalach wymiarowych poniżej nanometrów) cząstki przestają mieć charakter korpuskularny i opisywane są tzw. funkcjami falowymi, których kwadraty modułów określają gęstości prawdopodobieństwa. W takim ujęciu cząstki rozmywają się w przestrzeni w postaci właśnie chmur gęstości prawdopodobieństwa ich pomiaru położenia przestrzennego (wynika to z rozmycia trajektorii według zasady nieoznaczoności, co może być różnie interpretowane, np. jako poruszanie się cząstek po nieskończenie wielu trajektoriach jednocześnie w jednej rzeczywistości zgodnie z propozycją Feynmana, lub np. jako manifestacja tzw. wieloświatów, równoległych rzeczywistości według propozycji Everetta dla interpretacji mechaniki kwantowej). Niezależnie od interpretacji (nieweryfikowalnej fizycznie), podleganie układów nanoskopowych dynamice kwantowej powoduje nieklasyczne zachowanie się elektronów, opisywanych w mechanice kwantowej za pomocą tzw. funkcji falowych, których kwadraty modułów określają jedynie gęstości prawdopodobieństwa lokalizacji elektronów w przestrzeni, co wprowadza losowość (delokalizacja, efekty interferencyjne, tunelowanie przez bariery potencjałów).

Kwantowy szum (do którego istotny wkład wnosi np. tunelowanie kwantowe elektronów między ścieżkami układów scalonych przy nano-skalowych rozdzielczościach ich miniaturyzacji, w której kwantowe rozmycie gęstości prawdopodobieństwa elektronów obejmuje swoim zasięgiem różne ścieżki układu) przekłada się na właściwą (kwantową) składową szumu napięcia wyjściowego (np. na kondensatorze), które może być następnie w odpowiedni sposób próbkowane dla generowania (ekstrakcji) prawdziwie losowych ciągów binarnych (tj. liczb prawdziwie losowych w reprezentacji binarnej).

Poniżej przedstawiono skrótową analizę wyników badawczych w kierunku określenia optymalnego procesu kwantowego dla generacji losowości w zintegrowanym i praktycznym układzie QRNG (szczegółowa analiza znajduje się w publikacji P-4 oraz w szeregu pozostałych publikacji specjalistycznych i zbiorów danych źródłowych wskazanych powyżej i stanowiących wyniki realizacji etapu nr 2 projektu).

Kwantowa generacja losowości w oparciu o szum śrutowy

Szum śrutowy to w ogólności kwantowy rodzaj tzw. białego szumu (tj. szumu o całkowicie płaskim widmie, którego nazwa wywodzi się z analogii do widma fali elektromagnetycznej – światło białe może być traktowane jako szum e-m nałożenia się wszystkich długości fal – reprezentujących kolory – o całkowicie płaskim widmie w zakresie widzialnego spektrum fali elektromagnetycznej), który można dobrze modelować statystycznym rozkładem Poissona w dziedzinie czasowej.

W elektronice szum śrutowy wywodzi się bezpośrednio z fundamentalnie dyskretnej natury ładunku elektrycznego (mimo, że ładunek elementarny występuje w klasycznej elektrodynamice, tj. jest on

cechą fundamentalną w istocie kwantowego układu jakim jest elektron – cząstka elementarna). Szum śrutowy występuje jednak także w zjawiskach absorpcji fotonów w układach optycznych, gdzie jest wówczas związany ze skwantowaną naturą fali elektromagnetycznej, tj. światła w postaci fotonów.

Szum śrutowy jest więc efektem czysto kwantowym, wynikającym z fundamentalnych praw mechaniki kwantowej, które dotyczą dowolnych cząstek elementarnych, w tym zarówno elektronów jak i fotonów (choć w przypadku fotonów brakuje jeszcze pełnej teorii tzw. relatywistycznej mechaniki kwantowej, uwzględniającej efekty relatywistyczne wynikające ze stałości prędkości światła i związku czasoprzestrzennych z grawitacją oraz wyjaśnienia problematyki naruszenia zasady lokalności przez splątanie kwantowe, co z kolei zaburza związki przyczyno-skutkowe). Niezależnie od obecnych braków teoretycznych w obszarze podstawowym procesy fizyczne emisji i absorpcji światła są dobrze opisane tzw. złotą regułą Fermiego przejść kwantowych (tu przejść optycznych) i stanowią powszechny standard metodologiczny w mechanice kwantowej (należy podkreślić, że unifikacja teorii oddziaływań elektromagnetycznych z mechaniką kwantową została zrealizowana w zakresie tzw. teorii elektrodynamiki kwantowej).

Z szumem śrutowym w przypadku fotonów mamy do czynienia, gdy fotonów jest niewiele (np. w silnie tłumionej wiązce laserowej) i fundamentalnie kwantowe fluktuacje w ich emisji wpływają w sposób możliwy do wykrycia na fluktuacje intensywności wiązki (niewielkich zmian jej jasności), która odzwierciedla wtedy właśnie szum śrutowy (pojęcie to wprowadził w podobnym eksperymencie związanym z fluktuacjami prądu w lampach próżniowych w 1918 rok W. Schottky). Komponenta szumu śrutowego może być dominująca gdy liczba cząstek elementarnych podlegających prawom mechaniki kwantowej i przenoszących energię (np. elektronów w układzie scalonym lub fotonów w układzie optycznym) jest na tyle niewielka, by fluktuacje wynikające z rozkładu Poissona, opisującego występowanie niezależnych zdarzeń losowych (tj. dobrze modelujących procesy kwantowe), miały znaczenie będąc łatwo mierzalnymi.

Należy podkreślić, że pomimo, iż intensywność szumu śrutowego wzrasta jak pierwiastek kwadratowy wartości oczekiwanej liczby zdarzeń (np. emisji lub absorpcji elektronowych lub fotonowych, przy czym elektronowe, tzw. stopnie swobody odnoszą się do wzbudzeń i relaksacji energetycznych), to jednak efektywnie szum śrutowy szybko staje się coraz mniej istotny, ponieważ wielkość samego sygnału rośnie szybciej niż w zależności pierwiastkowej i w konsekwencji w proporcji względnej intensywność szumu śrutowego maleje, a stosunek sygnału do szumu, uwzględniając tylko szum śrutowy, wzrasta. Stąd szum śrutowy (np. w układach elektronicznych) jest generowany do ew. zastosowań jedynie przy małych prądach lub niskich natężeniach światła, tak aby później w odpowiedniej obróbce sygnałów podlegać wzmocnieniu. Aby możliwie najlepiej zapewnić reżim kwantowy w danym zjawisku fizycznym, najlepiej organizować je w zakresie dynamiki pojedynczych stanów kwantów (np. pojedynczych fotonów, które padając na półprzewodnik wzbudzają pojedyncze elektrony w pełni zgodnie z prawami mechaniki kwantowej). Wiąże się to

jednak z poważnymi trudnościami implementacyjnymi (zarówno w zakresie źródeł pojedynczych stanów kwantowych jak i ich detekcji).

Przykładowo w zakresie fotoniki, źródła jednofotonowe to np. silnie tłumione lasery (lub diody emisyjne), lub specjalistyczne układy optyki kwantowej, w których można wytworzyć fotony splątane polaryzacyjnie, a prawa mechaniki kwantowej gwarantują, że w danym (splątanym) stanie kwantowym takiego typu (tzw. stan Bella, maksymalnie splątany przez swoją symetrię) istnieje tylko para fotonów, które można rozdzielić przestrzennie w różnych drogach optycznych. Problem detekcji pojedynczych fotonów jest z kolei o tyle trudny, że fluktuacja prądu spowodowana pojedynczymi wzbudzeniami elektronowymi w efekcie fotoelektrycznym np. w złączu półprzewodnikowym typu p-n jest zbyt mała aby być bezpośrednio mierzoną (w tym celu stosuje się tzw. fotodiody lawinowe, w którym wzmacnia się jednoelektronowy sygnał poprzez jego zwielokrotnienie silnym polem elektrycznym (duże napięcie wsteczne, tj. przykładane przeciwnie do kierunku przewodzenia diody, o wartości często przekraczającej napięcie przebicia złącza) polaryzującym złącze i rozpędzającym wzbudzone w efekcie elektrycznym elektrony do energii, która powoduje wybijanie przez nie kolejnych elektronów ze złącza (także rozpędzanych przez silne polaryzację i wybijających kolejne elektrony) w efekcie lawinowym, od którego nazwę bierze tego typu detektor.

Odnośnie właściwości statystycznych szumu śrutowego, należy podkreślić, że w przypadku dużych liczb (np. odnoszących się do dużej liczby zjawisk elementarnych, w których mimo kwantowej natury poszczególnych podukładów, np. cząstek elementarnych – elektronów lub fotonów, ich ogromna liczba zaczyna zachowywać się klasycznie) rozkład Poissona zbliża się do rozkładu normalnego wokół swojej średniej, a zdarzenia elementarne (np. emisje/absorpcje fotonów, wzbudzenia/relaksacje elektronów, etc.) nie są już możliwe do indywidualnej detekcji, co przekłada się na trudność obserwacji szumu śrutowego w rzeczywistych pomiarach (ponieważ szum śrutowy staję się wtedy nieodróżnialny od zwykłego szumu charakteryzowanego rozkładem Gaussa, wynikającym z centralnego twierdzenia granicznego i prawa wielkich liczb w teorii prawdopodobieństwa). Wobec powyższego, gdy liczba zdarzeń elementarnych jest bardzo duża, wówczas stosunek sygnału do szumu jest także bardzo duży, i w tej sytuacji względne fluktuacje z większym prawdopodobieństwem będą spowodowane innymi (np. kolektywnymi, które przy angażowaniu odpowiednio dużej liczby stopni swobody zaczynają manifestować dynamikę klasyczną) zjawiskami, jednocześnie dominując nad trudną wówczas do wyodrębnienia komponentą szumu śrutowego.

O ile jednak pozostałe źródła szumu da się np. wystabilizować w określonych implementacjach układów fizycznych (np. w zakresie relatywnie stałego szumu termicznego w odpowiednio izolowanych układach) lub też narastają one wolniej niż szum śrutowy (proporcjonalny do pierwiastka z liczby zdarzeń elementarnych), to zwiększając liczbę zdarzeń elementarnych (tj. zwiększając np. napięcie prądu lub intensywność światła) można w takich układach doprowadzić do dominacji komponenty szumu śrutowego nad innymi komponentami fluktuacji sygnału.

Dodać tu można, że problematyka przejścia dynamiki kwantowej w klasyczną nie jest w pełni zrozumiana teoretycznie i stanowi istotny problem dla nieudanej dotychczas unifikacji teorii mechaniki kwantowej z klasycznym relatywizmem (szczególną i ogólną teorią względności). Łączy się to z problemem pomiaru kwantowego (a także takimi jak rola obserwatora w pomiarze kwantowym), który w tradycyjnym ujęciu mechaniki kwantowej jest postulowany jako aksjomat według schematu kolapsu funkcji falowej von Neumanna. Nowsze próby wyjaśnienia tego zagadnienia wykazują jak oddziaływanie (splątywanie się) ogromnej liczby stopni swobody układów (np. w konfiguracji doplątywania się stopni swobody makroskopowego przyrządu pomiarowego do stopni swobody układu kwantowego) prowadzi do kolapsu funkcji falowej (jest to tzw. *superwybór*, który jednak nie w pełni wyjaśnia dynamikę pomiaru kwantowego, z uwagi na ograniczenia nierelatywistyczne mechaniki kwantowej). W kontekście ww. modeli, przyjmuje się, że granica rzeczywistości klasycznej wyraża się w złożonościach układów (które oczywiście zależą od ich skali wymiarowej) – a limit tej złożoności wyraża stała Avogadra (określająca liczbę cząstek elementarnych w molu materii, która jest rzędu 10^{23}), choć trzeba podkreślić, że w zależności od układu, efekty kwantowe relatywnie minimalizują się (stają się nieistotne) już przy znacznie mniejszych (nawet o wiele rzędów) złożonościach układów (co np. było przedmiotem dokładnej analizy w zakresie kolektywnej dynamiki drgań cieczy elektronowej w nanocząstkach, tj. w zakresie teorii nano-plazmoniki, która to dziedzina zgodnie z założeniami projektu także była przedmiotem badań w zakresie kwantowej generacji losowości, co jest opisane szczegółowo w kolejnych akapitach). W projekcie rozwija się rozważania podejścia do kwantowych losowych efektów w obszarze poddyfrakcyjnej nano-fotoniki plazmonowej, co być może udałoby się zastosować do optyczne realizacji QRNG wcześniej nierozpatrywanej.

Dobrym przykładem układu eksperymentalnego dla badania szumu śrutowego jako kwantowego generatora losowości jest obwód elektroniczny obejmujący oświetlaną fotodiodę (aby takie źródło losowości było kwantowe zgodnie z powyższą argumentacją, należy mieć na uwadze, że również źródło fotonów, padających na fotodiodę powinno być kwantowe, tj. emitować niewielkie liczby fotonów, a najlepiej pojedyncze fotony). Z uwagi na obowiązywanie zasady nieoznaczoności pojedyncze fotony padające na półprzewodnikową fotodiodę (będąc absorbowanymi w paśmie walencyjnym) wytwarzają szum śrutowy w obwodzie o naturze kwantowej, czego dokładny opis teoretyczny zgodny z eksperymentem jest możliwy np. w zastosowaniu metody złotej reguły Fermiego.[1] Wybór odpowiedniej komponenty szumu kwantowego z ogólnego sygnału szumu, którego wykorzystanie jest możliwe dla generacji liczb prawdziwie losowych nie jest trywialną operacją, jednak rekompensuje to relatywnie nieskomplikowana architektura źródła losowości w pełni zbieżna z rozwiniętym w zakresie miniaturyzacyjnym oraz integracyjnym technologicznym zaawansowaniem nanoelektroniki układów scalonych. Jednak energia szumu śrutowego nie zawsze

[1] Trzeba tu podkreślić, że efekt opisywany przez złotą regułę Fermiego jest kwantowy – reguła ta daje prawdopodobieństwo przejścia kwantowego na jednostkę czasu i to prawdopodobieństwo ma ten sam bezwzględny losowy atrybut co losowy wynik rzutowania von Neumanna. Wyniki prac badawczych wskazuję też, że wykorzystanie tej losowości (źródła entropii) do układu generacji losowości kwantowej QRNG jest znacznie bardziej praktyczne niż implementacja rzutowania von Neumanna (analiza przedstawiona w publikacji P-5).

jest dobrze rozłożona w całym paśmie będącym przedmiotem zainteresowania. Architektura układu kwantowego generatora losowości opartego na fotodiodzie w istocie wykorzystuje efekt fotoelektryczny (tu złota reguła Fermiego) i w tym zakresie powoduje częściowe przekrycie koncepcyjne z kolejnym rozdziałem (dotyczącym zjawiska fotoelektrycznego jako podstawy generacji losowości), jednak szum śrutowy w układach elektronicznych (np. silnie zminiaturyzowanych układach scalonych), może wynikać także z innych kwantowych zjawisk dotyczących dynamiki elektronów i ich np. tunelowania.

Istotną kwestią w zakresie badań przemysłowych nad szumem śrutowym jako źródłem generacji losowości jest rozkład energii szumu (zależny od napięcia elektrycznego i impedancji w układzie, przy czym pożądany jest możliwie płaski rozkład w szerokim spektrum, który w przypadku mocno szczytowych rozkładów energii w określonych układach wymaga zaawansowanego filtrowania). Przykładowo źródłem szumu śrutowego może być wzmacniany kwantowy sygnał elektronowy wytwarzany na tranzystorze spolaryzowanym zaporowo (emiter jest nasycony elektronami, które kolejno losowo w zakresie ich fundamentalnej dynamiki kwantowej przechodzą przez pasmo wzbronione). Ten słaby sygnał prawdziwie kwantowy jest następnie wzmacniany przez kilka kolejnych tranzystorów, a wynik jest przekazywany do tzw. wyzwalacza Schmitta (obwód komparatora z histerezą implementowaną przez dodatnie sprzężenie zwrotne do nieodwracającego wejścia komparatora lub wzmacniacza różnicowego – jest to zatem układ aktywny, który przekształca analogowy sygnał wejściowy na cyfrowy sygnał wyjściowy). W wyzwalaczu Schmitta (nazywanym tak ponieważ wyjście zachowuje swoją wartość, dopóki wejście nie zmieni się na tyle, aby wywołać zmianę) w konfiguracji nieodwracającej, gdy wejście ma wyższą wartość napięcia elektrycznego niż określony próg, na wyjściu również jest wysoka wartość napięcia. Gdy wejście z kolei jest poniżej innego (niższego) określonego progu napięcia, wówczas wyjście również ma niską wartość napięcia. Natomiast podczas gdy napięcie na wejściu znajduje się (odpowiednio obniżając się lub podnosząc) pomiędzy dwoma ww. określonymi poziomami, wyjście zachowuje swoją wcześniejszą wartość. Takie działanie podwójnego progu to histereza, która sprawia, że wyzwalacz Schmitta realizuje prosty rodzaj pamięci binarnej i może działać jako tzw. przerzutnik logiczny. Główną rolą wyzwalacza Schmitta jest właśnie filtrowanie sygnału w celu usunięcia szumu z sygnałów występujących w obwodach elektronicznych. Tego typu rozwiązanie może być wykorzystywane także w filtrowaniu niepożądanego typu szumu, tak aby wyodrębnić jedynie szum czysto kwantowy. Rozkład Poissona dla elektronowego szumu śrutowego wprowadzony w 1918 roku przez Schottky'ego jest przybliżeniem klasycznym, nie uwzględniającym obowiązującej elektrony kwantowej statystyki Fermiego-Diraca. Właściwy rozkład uwzględniający statystykę kwantową elektronów i ich pomiarów w temperaturze zera absolutnego został uzyskany dopiero w latach 90 (przez Khlusa, Lesovika i niezależnie przez Büttikera). Szum ten jest biały (nie zależy od częstotliwości) i zawsze stłumiony względem wartości z rozkładu Poissona (współczynnik tego tłumienia nazywany jest współczynnikiem Fano). Należy podkreślić, że szum śrutowy z różnych kanałów transportu elektronowego jest całkowicie niezależny.

Przykładami różnych (w tym skrajnych) konfiguracji szumu śrutowego w układach elektronicznych mogą być np. złącza tunelowe (charakteryzujące się bardzo niską transmisją we wszystkich kanałach transportu elektronowego, dlatego przepływ elektronów jest poissonowski, a współczynnik Fano równy jeden), punktowe styki kwantowe (charakteryzowane idealną transmisją we wszystkich kanałach transportowych, co powoduje brak szumów i współczynnik Fano równy zero), czy też np. dwuwymiarowy gaz elektronowy, w którym występuje kwantowy ułamkowy efekt Halla, w którym prąd elektryczny jest przewodzony przez poruszające się na krawędzi próbki nie w pełni wyjaśnione kwaziczą stki (proponowany w literaturze fikcyjny model złożonych fermionów jak się okazuje może być zastąpiony nowymi modelami w zakresie teorii grup warkoczowych w topologii – tu prace jednego z realizatorów projektu, Jacak, J. E. 2021, Annals of Physics, 430, 168493) w uproszczeniu o wymiernie ułamkowym ładunku elektronu (przy czym pierwszym eksperymentalnym pomiarem ich ładunku był szum śrutowy, historycznie wykorzystywany także wcześniej w eksperymentach pierwotnie wyznaczających ładunek elementarny elektronu).

Kwantowa generacja losowości w oparciu o efekt fotoelektryczny

Badania generacji losowości w kwantowym efekcie fotoelektrycznym (przy emisji fotonów w wiązce koherentnej lasera lub półprzewodnikowej diody) sprowadzają się do badań detekcji pojedynczych fotonów.

Jak wyjaśniono w powyższym akapicie w istocie zjawiska fotonowe w efekcie fotoelektrycznym także dotyczą szumu śrutowego w zakresie absorpcji oraz emisji pojedynczych fotonów (zamiast odpowiednio wzbudzeń oraz relaksacji elektronów, czy też w kategoriach ich przechodzenia między pasmami w złączu p-n, tj. w istocie wybijania elektronów w obszarze złącza i ich przejściu bariery potencjału złącza, i szczeliny wzbronionej między pasmami walencyjnym i przewodnictwa, to także może być interpretowane jako emisja odnośnie wzbudzenia i później rekombinacji wzbudzonego ekscytonu, tj. pary elektron-dziura (elektron pozostawia w pasmie walencyjnym dziurę i poprzez przerwę wzbronioną obydwa nośniki tworzą parę mniej lub bardziej związaną – ekscyton niestabilny w czsie). Wszystkie te efekty, tj. emisje/absorpcje fotonów i wzbudzenia/relaksacje elektronów-dziur są ze sobą bezpośrednio powiązane i są całkowicie kwantowe i wyrażają fundamentalne sprzężenie światła i materii i mogą być wykorzystane jako źródło entropii w QRNG.

Należy zatem podkreślić, że w fizyce kwantowej (czy precyzyjniej w elektrodynamice kwantowej) występuje zjawisko sprzężenia światła i materii poprzez sprzężenie elektrycznej komponenty fali e-m fotonu z ładunkiem elektrycznym nośnika (elektronu lub dziury). Każdorazowo wzbudzenie energetyczne elektronu (dziury) wiąże się z absorpcją fotonu (kwantu energii), podczas gdy relaksacja elektronu związana jest z emisją fotonu (co wypełnia zasadę zachowania energii wynikająca z jednorodności czasu). Wzbudzany elektron pozostawia dziurę w paśmie walencyjnym, w który staje

się ona efektywnym nośnikiem dodatniego ładunku elementarnego i także przewodzi prąd (tzw. prąd dziurowy w półprzewodnikach).

W ujęciu bardziej fundamentalnym i ogólnym, sprzężenie światło-materia dotyczy zjawisk kreacji i anihilacji materii i antymaterii (jak opisuje to kwantowa elektrodynamika Diraca). Para cząstka-antycząstka może zostać wykreowana przez absorpcję fotonu gamma o bardzo wysokiej energii determinowanej przez słynne równanie ogólnej teorii względności $E=mc^2$ opisującej pełny zamianę masy w energię (unoszonej przez fotony, tj. kwanty fali elektromagnetycznej o odpowiedniej częstości czy długości fali, zgodnie z zasadami zachowania energii i pędu). Spotkanie cząstki z antycząstką kończy się anihilacją, w której cała masa zamienia się na energię w postaci emitowanego fotonu gamma (a w istocie dwóch fotonów gamma emitowanych w przeciwnych kierunkach w linii prostej, tak aby wypełnić tym zasadę zachowania pędu).

W układach półprzewodnikowych efekt fotoelektryczny można interpretować jako efektywny model ciałostałowy ww. fundamentalnego procesu w elektrodynamice kwantowej, w którym można mówić o efektywnej kreacji pary elektron-dziura (dziura zachowuje się efektywnie jak antyelektron, odpowiednik pozytronu, w strukturze pasmowej półprzewodnika). Swoisty proces kreacji pary elektron-dziura (wzbudzenia elektronu do wyższego pasma walencyjnego, po którym elektron ten dołącza do cieczy elektronowej przewodzącej prąd w paśmie przewodnictwa) jest zjawiskiem kwantowym, w którym dochodzi do absorpcji fotonu (efekt odwrotny polega na relaksacji wzbudzenia z pasma przewodnictwa do pasma walencyjnego -- rekombinacji ekscytonu, czemu towarzyszy z kolei emisja fotonu; rekombinacja może być też bezpromienista np. z udziałem fononów lub innych cząstek). Procesy te są procesami czysto kwantowymi, a ponadto ich dynamika warunkowana jest kwantową dystrybucją fotonów w źródle światła (np. wiązce laserowej o rozkładzie Poissona modelującym wzajemną niezależność zdarzeń elementarnych i przedziałów czasowych ich zachodzenia).

Należy podkreślić, że efekt fotoelektryczny jest także podstawą działania detektorów optycznych pojedynczych fotonów (np. diod lawinowych), dodając w procesach generacji losowości wynikających z innych fundamentalnie niedeterministycznych własności układów optyki kwantowej (np. w zakresie wyboru drogi optycznej fotonu po przejściu wiązki przez np. tzw. polaryzacyjny rozdzielacz wiązki, PBS) również tą dodatkową komponentę losowości kwantowej (wzmacniając źródło entropii).

W tym kontekście należy zauważyć, że w zakresie podstawowego podejścia do losowości opartej na efektach fotonicznych w układach optyki kwantowej zwykle wybiera się niedeterminizm przestrzenny, związany z nieokreślonością wyboru drogi optycznej przez fotony przechodzące przez zwierciadła półprzepuszczalne (najczęściej implementowane przez kostki światłodzielące, tzw. beamsplittery). Wykorzystanie niedetermizmu przestrzennego (wyboru drogi optycznej) wiąże się jednak z koniecznością wykorzystania co najmniej dwóch detektorów fotonów, tak by określać, która z dróg optycznych została losowo zrealizowana (poza tym układ optyczny wymaga odpowiedniej

kalibracji i jest wrażliwy na perturbacje mechaniczne wpływające na położenie przestrzenne komponentów optyki kwantowej, mogące wpływać na odchylenia od prawdziwej losowości i wprowadzać niepożądany silny bias). Tematyka ta jest rozwinięta w kolejnych akapitach analizujących układy optyki kwantowej jako źródła kwantowej losowości.

W zakresie losowości kwantowej opartej z kolei bezpośrednio na efekcie fotoelektrycznym (tj. na zjawiskach emisji i absorpcji fotonów w półprzewodniku) właściwym parametrem źródła losowości jest niedeterminizm w domenie czasowej, a nie przestrzennej. W takiej sytuacji w odpowiednim układzie wszystkie fotony poruszają się po tej samej drodze optycznej i mogą być rejestrowane tylko przez pojedynczy detektor (zamiast 2 detektorów wymaganych do odróżniania dróg optycznych).

Taki generator jest odporniejszy na zaburzenia mechaniczne mogące wpływać na odchylenia w kwantowym niedeterminizmie wyboru drogi optycznej. Ponadto ew. fluktuacje w zakresie sprawności źródła lub detektora nie powinny także powodować odchyleń w generowanej losowości, ponieważ nie wpływałyby na zmiany częstości rejestracji zliczeń kodujących losowe bity 0 i 1 (w układach, w których występują dwa detektory, ważne jest aby ich sprawność była taka sama. gdyż w stałym czasie działania generatora asymetryczne fluktuacje sprawności jednego detektora względem drugiego będą wprowadzać oczywiste odchylenie – bias). Cechy te (dotyczą układów opartych na efekcie fotoelektrycznym) pozwalają w dużym stopniu unikać konieczności złożonej kalibracji układu, a także zapewniają jego większą trwałość i odporność na perturbacje mechaniczne. Wadą takiego podejścia jest natomiast znacznie bardziej skomplikowana procedura ekstrakcji losowych bitów ze zdarzeń elementarnych (absorpcji fotonów w detektorze padających na jego powierzchnię w sposób niedeterministycznie losowy w reżimie kwantowej emisji pojedynczych fotonów z ich źródła) i wymaga dodatkowego przetwarzania elektronicznego sygnału.

Bit losowy w generowanym losowym ciągu binarnym w ramach efektu fotoelektrycznego powinien mieć absolutnie niedeterministyczną wartość 0 lub 1 (tj. wartość całkowicie niezależną od wyników generowanych na innych pozycjach losowego ciągu binarnego – oznacza to, że prawdopodobieństwa wygenerowania 0 oraz 1 wynoszą dokładnie 50% i są całkowicie niezależne).

W zakresie implementacji fizycznej wymaga to dysponowania kwantowym źródłem fotonów, które zapewni ww. sytuację (prawdopodobieństwa w pomiarze von Neumanna stanów czysto kwantowych w symetrycznych superpozycjach są od siebie całkowicie niezależne i wynoszą dokładnie 50%).

Sytuacja ta modelowana może być rozkładem statystycznym Poissona zdarzeń elementarnych (absorpcji fotonów przez detektor) względem czasu, który charakteryzowany jest tym, że odstępy czasowe pomiędzy kolejnymi zdarzeniami są całkowicie losowe (innymi słowy nie ma żadnej korelacji między tym czy interwały czasowe rejestracji kolejnych zdarzeń elementarnych są mniejsze czy większe względem poprzednich, a cały rozkład ma charakter wykładniczy).

W takim modelu ogólna metoda ekstrakcji losowych bitów odnosi się do porównywania nienakładających się losowych interwałów czasów między kolejnymi zdarzeniami elementarnymi (rejestracjami fotonów przez detektor). Przykładowa konwencja to określenie generowanego bitu losowego jako 0 w przypadku gdy poprzedni interwał czasowy jest mniejszy niż kolejny, oraz jako 1 w przeciwnym wypadku.

Ponieważ interwały czasowe oddzielające kolejne zdarzenia elementarne są od siebie całkowicie niezależne, prawdopodobieństwo, że poprzedni interwał czasowy jest mniejszy od kolejnego jest dokładnie takie samo jak prawdopodobieństwo odwrotnej sytuacji, tj. że kolejny interwał czasowy jest mniejszy od poprzedniego (prawdopodobieństwo to jest zatem równe dokładnie 50% i prowadzi do braku korelacji, co dotyczy całej serii zdarzeń elementarnych o kwantowej dystrybucji prawdopodobieństw modelowanej rozkładem Poissiona).

W powyższego wynika zatem, że tak zdefiniowany generator będzie generował losowe bity 0 lub 1 z takim prawdopodobieństwem na wszystkich pozycjach losowego ciągu binarnego z pełnym niedeterminizmem warunkowanym faktyczną niezależnością czasową okresów między kolejnymi zliczeniami zdarzeń elementarnych na detektorze fotonów (co wymaga jednak kwantowego źródła pojedynczych fotonów, np. silnie tłumionej wiązki laserowej). Wzajemna niezależność bitów (brak korelacji między pozycjami bitowymi w losowym ciągu) wynika z niezależności zdarzeń, która charakteryzuje zjawiska kwantowe i jest modelowana rozkładem Poissona.

Na marginesie można dodać, że uogólnienie powyższego modelu często próbuje się w literaturze stosować w odwrotnym kierunku, np. proponując użycie źródła nie w pełni kwantowego, np. diody LED emitującej ogromne liczby fotonów, zamiast pojedynczych (manifestujących statystykę kwantową), i wykazywaniem jednak istnienia statystyki rozkładu Poissona, która efektywnie może uzasadniać kwantowość źródła (w takiej sytuacji trzeba w odpowiedni sposób filtrować komponenty szumu klasycznego).

Dodać również należy, że powyżej opisane podejście do generacji losowości w efekcie fotoelektrycznym przekrywa się koncepcyjnie z zagadnieniem szumu śrutowego (jest to w istocie fotonowy szum śrutowy, w odróżnieniu od elektronicznego, jednak zgodnie z argumentacją przedstawioną w poprzednim paragrafie, w związku z fundamentalnym sprzężeniem materii i światła, oba te efekty są bezpośrednio powiązane, ponieważ np. 'emisje' – tj. wzbudzenia – elektronów w półprzewodniku, determinowane są przez absorpcje fotonów i odwrotnie).

Proponowana powyżej metoda ekstrakcji losowych wartości binarnych w zjawisku fotoelektrycznym jest skuteczna o ile układ rzeczywiście jest idealnie kwantowy. Należy podkreślić jednak, że implementacje fizyczne mogą wprowadzać (i realistycznie oczywiście zwykle wprowadzają) pewne, nawet niewielkie, ale jednak zawsze istotne fundamentalnie, odchylenia od kwantowości, które przekładają się na odchylenia od absolutnej losowości generowanego ciągu binarnego.

Należy podkreślić, że uzyskać wyidealizowaną sytuacją dynamiki kwantowej (lub nawet tylko do niej zbliżoną) jest bardzo trudno w rzeczywistych implementacjach fizycznych. Przykładowo impulsy laserowe o standardowych mocach (intensywnościach światła) zawierają ogromne liczby fotonów i przez to nie realizują rozkładu statystycznego Poissona modelującego reżim praw mechaniki kwantowej dla zdarzeń elementarnych odpowiadających emisjom fotonowym koherentnego źródła (tj. w pełni niezależnych w domenie czasowej).

W przypadku gdy w impulsach laserowych mamy do czynienia z dużą liczbą fotonów statystyka czasowa sprowadza się do rozkładu normalnego (Gaussa). Wynika to z centralnego twierdzenia granicznego i prawa wielkich liczb: jeśli dowolna wielkość jest średnią bardzo wielu czynników losowych to niezależnie od rozkładu statystycznego tych czynników łączny rozkład tej wielkości będzie dążył do rozkładu gaussowskiego.

Statystyka poissonowska światła jest wyznacznikiem koherencji kwantowej jego źródła, podczas gdy statystyka gaussowska wykazuje brak tej koherencji, a sprowadza się do liczby kwantów światła fotonów (dla zaistnienia modelu statystyki poissonowskiej konieczne są bardzo niewielkie liczby fotonów, a wzrost ich liczby powoduje przechodzenie statystyki w kierunku rozkładu normalnego).

Przeciwdziałaniem dużej liczbie fotonów w impulsie laserowym może być silne tłumienie wiązki (nawet takie, które w większości impulsów pozostawia zerową liczbę fotonów, czyli efektywnie prawie całkiem wytłumia źródło, jednak pozostawia niewielkie prawdopodobieństwo transmisji pojedynczego fotonu w impulsie, co manifestuje się raz na wiele impulsów, ale jeśli tych impulsów jest bardzo wiele, jak np. w laserze femtosekundowym, tj. rzędu 10^{15} impulsów na sekundę, wówczas nawet silne tłumienie pozostaje w zasięgu praktycznej realizacji zapewniającej odpowiednie częstotliwości generacji losowych ciągów binarnych).

Jest to znany problem w zakresie komunikacji kwantowej, w którym silne tłumienie źródła ma tą wadę, że obniżając jego intensywność wpływa się negatywnie na zasięg komunikacji, jednak w zintegrowanych układach kwantowej generacji liczb losowych QRNG nie jest to zasadniczym problemem (koherentne źródło pojedynczych fotonów w takich układach powinno znajdować się w zasadzie w bezpośrednim pobliżu detektora). Poza tłumieniem impulsów laserowych zasadniczo najlepszym rozwiązaniem gwarantującym w pełni kwantową statystykę, tj. pojedyncze fotony, jest wykorzystanie splątania kwantowego, które w procesie parametrycznej konwersji w dół (SPDC) będzie szerzej omówione w zakresie wykorzystania układów optyki kwantowej do generacji prawdziwej losowości w oparciu o niedeterminizm przestrzenny (także jednak częściowo przekrywając się z niniejszym obszarem w zakresie zjawiska fotoelektrycznego powodującego nie determinizm w domenie czasowej).

Podsumowując, problemy związane ze źródłami są istotne, ale mogą być do pewnego pokonane przy wykorzystaniu zaawansowanych technik optyki kwantowej (np. procesu SPDC generacji splątania kwantowego na polaryzacjach fotonów w nieliniowym procesie elektrodynamicznym np. w silnie

dwójłomnych kryształach BBO). Prowadzi to jednak do konsekwencji polegającej na tym, że sam prosty efekt fotoelektryczny, nie jest już odosobnionym mechanizmem fizycznym podlegającym prawom mechaniki kwantowej możliwym do wykorzystania w zintegrowanym generatorze liczb losowych, a staje się częścią znacznie bardziej zaawansowanego obszaru optyki kwantowej.

W tym też aspekcie prowadzono badania empiryczne rozszerzające problematykę samego efektu fotoelektrycznego jako źródła losowości kwantowej do bardziej uogólnionej optyki kwantowej z włączeniem niedeterminizmu w domenie przestrzennej, także przy wykorzystaniu splątania kwantowego (co ponadto daje bardzo ważną możliwość w pełni obiektywnej weryfikacji faktycznej kwantowości procesu poprzez weryfikację złamania nierówności Bella/CHSH na klasyczne, tj. lokalne limity korelacji wyników pomiarów, co również było przedmiotem empirycznych badań laboratoryjnych w toku realizacji II etapu projektu, dla celów wykazania prawdziwej kwantowości zjawiska, fundamentalnie naruszającego zasadę lokalności obowiązującą w fizyce klasycznej – więcej informacji w publikacji P-7).

W zakresie zjawiska fotoelektrycznego (także jako składowej szerszej dziedziny procesów optyki kwantowej) należy zwrócić jeszcze uwagę na problematykę detekcyjną (wykrywanie pojedynczych fotonów realizujących dynamikę kwantową).

Odnośnie kwestii korelacji, należy zauważyć przede wszystkim rolę tzw. martwego czasu działania detektora fotonowego (lub tzw. okien detekcyjnych, oddzielonych refrakcyjnymi okresami nieaktywności detekcyjnej, tj. właśnie martwego czasu detektora). Aby rejestrować zdarzenia elementarne (preferencyjnie związane z pojedynczymi absorpcjami fotonowymi, które wówczas z całą pewnością realizowane są w reżimie mechaniki kwantowej i w konsekwencji wprowadzają pełny niedeterminizm w zakresie schematu pomiaru von Neumanna) należy wykorzystywać detektor jednofotonowy. Problemem rozwiązywanym przez detektory jednofotonowe jest wzbudzanie na tyle silnego sygnału (np. elektronowego), aby można było ten sygnał odczytać w makroskopowy sposób jako wynik pomiaru (tj. zdarzenie rejestracji pojedynczego fotonu o niewspółmiernie małej energii względem koniecznej skali energetycznej odczytywalnego sygnału pomiarowego). Wymaga to udziału ogromnej liczby stopni swobody, jak się przyjmuje rzędu stałej Avogadra tj. 10^{23}, w których to stopniach swobody układu pomiarowego kodowany jest możliwy do odczytania w sensie klasycznym wynik pomiaru (w schemacie ewolucji unitarnej układu mierzonego – fotonu – oraz układu pomiarowego – detektora, zawsze ostatecznie makroskopowego, jest wspólna ewolucja, która prowadzi do kwantowego splątania się stopni swobody układu mierzonego z układem pomiarowym). Dalej, zgodnie z argumentacją tzw. superwyboru, następuje całkowite defazowanie macierzy gęstości co odpowiada realizacji kolapsu von Neumanna, tj. pomiaru kwantowego – w mechanizmie zaproponowanym jako teoretyczne wyjaśnienie kolapsu von Neumanna postulowanego wcześniej w mechanice kwantowej (ogromna krotność całek realizujących iloczyny skalarne funkcji falowych całego układu złożonego obejmującego układ mierzony i przyrząd pomiarowy, rzędu co najmniej liczby Avogadro, nawet jeśli całki te są tylko nieznacznie różne od 1 – co jest konieczne aby przyrząd

pomiarowy w wymiarowej skali klasycznej mógł pokazać różnicę w wyniku pomiaru, tj. zarejestrowania lub braku zarejestrowania fotonu – prowadzi do zerowania się elementów pozadiagonalnych macierzy gęstości i właśnie do jej pełnego defazowania, ponieważ iloczyn – calka wielokrotna – nawet niewiele mniejszych od 1 czynników jest praktycznie równy 0).

By taki schemat działania miał miejsce w detektorze jednofotonowym, trzeba w odpowiedni sposób zaprojektować oddziaływanie fizyczne, które będzie w stanie splątać stopnie swobody układu kwantowego z ogromną liczbą stopni swobody makroskopowego układu pomiarowego (tak też dzieje się np. w fotodiodzie lawinowej, APD). Jednofotonowa dioda lawinowa jest najczęstszą i obecnie najlepszą znaną implementacją detektora jednofotonowego (choć te są intensywnie rozwijane np. w zakresie nano-wnęk rezonansowych).

Fotodioda lawinowa bezpośrednio wykorzystuje efekt fotoelektryczny do transformacji światła w przepływ elektronów nazywany fotoprądem. Główne zastosowania fotodiody lawinowej dotyczą właśnie kwantowych pomiarów pojedynczych fotonów w optyce kwantowej, w tym w kryptografii kwantowej i szerzej w komunikacji kwantowej wykorzystującej nisko energetyczne fotony, najczęściej w okolicach widma widzialnego (ale także fotonów o wysokich energiach, np. fotonów gamma w pozytonowej tomografii emisyjnej, opartej na zjawisku anihilacji materii z antymaterią w rozpadzie beta substancji radioaktywnej, np. napromieniowanej glukozy, szybko akumulowanej w guzach nowotworowych w celu ich detekcji we wczesnym stadium w urządzeniu PET).

Konstrukcja fotodiody lawinowej opiera się na półprzewodnikowym złączu typu p-n z warstwą zaporową. Fotony padające na złącze p-n w zjawisku efektu fotoelektrycznego prowadzą do wzbudzeń elektronowych (można mówić o ich emisjach ze złącza), generując fotoprąd. Gdy są to pojedyncze fotony, wzbudzenia powodowane przez nie w zakresie pojedynczych tylko elektronów pozostają poza możliwościami rozdzielczymi próbkowania zmian natężenia lub napięcia w obwodzie elektrycznym. Zmienić można to poprzez silną polaryzację złącza bardzo wysokim napięciem wstecznym. Polaryzacja taka wytwarza silne pole elektryczne, w którym pojedyncze wzbudzone elektrony emitowane ze złącza uzyskują bardzo dużą energię i wybijają w lawinowej reakcji kolejne elektrony ze złącza (podobnie jak ma to miejsce w reakcji łańcuchowej).

Prowadzi to do znacznego wzmocnienia fotoprądu pierwotnie generowanego ze zdarzeń elementarnych do wartości które są klasycznie mierzalne (w zakresie nawet kilku rzędów wielkości, co determinowane jest przyłożonym napięciem elektrycznym polaryzującym złącze p-n). Wysokie wartości napięcia wstecznego, tj. przyłożonego przeciwnie do kierunku przewodzenia złącza (jeśli powyżej 1000-1500V przekraczając napięcie przebicia złącza, nazywane właśnie jednofotonowymi fotodiodami lawinowymi, tj. single-photon avalanche diodes, SPAD) są konieczne do rejestrowania pojedynczych fotonów, a reakcja lawinowa wzbudzania kolejnych elektronów ze złącza wzmacniająca pierwotny fotoprąd np. o 6 rzędów, jest w istocie realizacją schematu superwyboru w pomiarze kwantowym prowadzącym do pełnego defazowania macierzy gęstości w realizacji pomiaru

kwantowego, poprzez splątanie ogromnej liczby stopni swobody układu pomiarowego z mierzonym. Dwa najważniejsze parametry jednofotonowych diód lawinowych to ich wydajność kwantowa (opisująca poziom absorpcji padających fotonów, które wzbudzają elektrony) oraz tzw. całkowity prąd upływu, będący sumą prądu ciemnego (niewielkiego prądu, który płynie w układzie nawet w sytuacji braku absorpcji jakichkolwiek fotonów), fotoprądu i szumu. Szum elektroniczny można podzielić na szum szeregowy i równoległy. Szum szeregowy, który jest efektem szumu śrutowego, jest proporcjonalny do pojemności fotodiody lawinowej, podczas gdy szum równoległy jest związany z fluktuacjami prądów objętościowych i powierzchniowych fotodiody. Innym źródłem szumu jest współczynnik nadmiaru szumu (ENF). Współczynnik ten ma charakter multiplikatywnej poprawki w zakresie istniejącego szumu, która opisuje poziom wzrostu szumu statystycznego, a w szczególności szumu Poissona, spowodowanego procesem zwielokrotnienia elektronicznego. ENF jest określony dla dowolnego układu elektronicznego, który zwielokrotnia sygnał (np. fotopowielacz czy właśnie dioda lawinowa) i jest często określany mianem szumu wzmocnienia (zależnym od wielkości wzmocnienia i wyrażonym przez stosunek szybkości jonizacji zderzeniowej dziur w paśmie walencyjnym do szybkości jonizacji zderzeniowej elektronów w paśmie przewodnictwa – przy czym w standardowym trybie pracy układu detekcyjnego pożądana jest znaczna asymetria między tymi dwiema szybkościami, aby minimalizować ENF jako czynnik ograniczający możliwą rozdzielczość energetyczną układu, podczas gdy w zastosowaniach generacji losowości, komponenta ta może być dodatkowym źródłem losowości poza efektem fotoelektrycznym w zakresie niezależnych kanałów elektronicznego szumu śrutowego (który opisano we wcześniejszych paragrafach).

Podobnie jak w szumie śrutowym, ogólny szum w układzie fotodiody lawinowej powinien uwzględniać również omawiany wcześniej współczynnik Fano (poprawkę multiplikatywną do szumu śrutowego w rozkładzie statystycznym Poissona wynikającą z konwersji energii przekazywanej przez naładowaną cząstkę do wzbudzanej pary elektron-dziura, tj. w zakresie sygnału elektrycznego przed jego zwielokrotnieniem). Współczynnik korygujący opisuje spadek szumu w stosunku do statystyki Poissona, spowodowany jednorodnością procesu konwersji i brakiem (lub też słabym poziomem) sprzężenia z innymi stopniami swobody półprzewodnika w procesie konwersji, np. wzbudzeń fonowych (wyidealizowany półprzewodnik zamieniałby energię naładowanej cząstki na konkretnie określoną i powtarzalną liczbę par dziur elektronowych realizując zasadę zachowania energii – w rzeczywistości jednak energia przekazana przez naładowaną cząstkę dzielona jest na wzbudzanie ekscytonów, ale także i fononów akustycznych oraz optycznych w sieci krystalicznej półprzewodnika i związane z tym promieniowanie cieplne czy też wprowadzenie perturbacji deformacyjnych i przemieszczeniowych). Istnienie wielu dodatkowych kanałów transferu energii (zwłaszcza oddziaływań tzw. orbitalnych stopni swobody wzbudzeń ładunkowych z morzem fononów, prowadzących do procesów ubierania się ekscytonów w tzw. polarony, efektywne cząstki powstałe w zakresie hybrydyzacji ze stopniami swobody fononów) wprowadza złożone procesy stochastyczne, w których dana ilość energii przekazywana w pojedynczym procesie zmienia się w zależności od zdarzenia, nawet jeśli ilość wnoszonej w zdarzeniu elementarnym energii jest zawsze stała.

Szczegółowa analiza zagadnień związanych z oddziaływaniem wzbudzeń elektronowych i dziurowych (ekscytonowych) w półprzewodnikach (zwłaszcza w kropkach kwantowych) wiąże się z procesami tzw. dekoherencji kwantowej w zakresie oddziaływań (hybrydyzacji) z fononami. Zaawnasowana analiza fizyczna tych efektów jest tematyką monografii członka zespołu projektowego W. A. Jacaka pt. „Dekoherencja orbitalnych i spinowych stopni swobody w kropkach kwantowych".

Fizyka kwantowa związana ze współczynnikiem szumu wzmocnienia i współczynnika Fano (szumu konwersji) jest bardzo złożona. Jednak abstrahując od konkretnych mechanizmów fizycznych fenomenologiczne zastosowanie tych czynników jako korekcji multiplikatywnych do oczekiwanego szumu o rozkładzie Poissona jest ogólnie przyjętą praktyką w elektronice. Oprócz problematyki szumów istnieją również istotne ograniczenia w działaniu fotodiod lawinowych APD (a zwłaszcza jednofotonowych diod lawinowych SPAD) dotyczące uwarunkowań czasowych działania tych układów (związanych z pojemnością, czasem przejścia i czasem zwielokrotnienia lawiny). Te czynniki wpływają właśnie na okres martwy działania detektora i determinują tzw. okna pomiarowe *(detection gates).* Przykładowo pojemność układu wzrasta wraz ze wzrostem powierzchni i zmniejszeniem grubości złącza. Czasy przejścia z kolei zarówno dla elektronów, jak i dziur zwiększają się wraz ze wzrostem grubości. Powoduje to swoistą konkurencję pomiędzy pojemnością a czasem przejścia dla ogólnej wydajności (minimalizacji czasów martwych). Czas zwielokrotnienia sygnału pierwotnego kwantowego fotoprądu w ramach lawiny elektronowej może być określony w przybliżeniu pierwszego rzędu przez iloczyn wzmocnienia i przepustowości. Im czulsze detektory (w granicy jednofotonowej) tym większy jest czas martwy ich działania (albo krócej trwające okno detekcyjne w stosunku do czasu następującej później dynamiki lawinowej), co może wpływać na wprowadzanie korelacji pomiarowych, zwłaszcza jeśli czas martwy po każdym wykryciu zdarzenia elementarnego nie ma stałej długości. Wynika to z następującej analizy: proces generowania losowych bitów wykorzystuje jedynie różnicę dwóch interwałów czasu aby określić, który był większy; ponieważ każdy losowy interwał czasowy między zdarzeniami zawierać może jednak czas martwy działania detektora, to o ile ten czas jest charakteryzowany zmienną długością trwania (np. skorelowaną z pewnymi parametrami działania układu) może wprowadzać odchylenia losowości opartej na tylko teoretycznej pełnej niezależności od siebie interwałów czasowych kolejnych detekcji w modelu rozkładu Poissona, w rzeczywistości zależnych jednak także od czasów martwych detektora.

Fluktuacje długości trwania czasów martwych detektora powinna być eliminowana na poziomie konstrukcji układu, ale wpływać może na nią np. nierównomierny rozkład intensywności silnie tłumionych impulsów laserowych (w niektórych impulsach mogą być pojedyncze fotony, a w innych całe ich ogromne grupy w tym samym stanie kwantowym z niezerowym prawdopodobieństwem). Reakcja lawinowa detektora SPAD może wówczas zależeć od tej liczby fotonów, które w większej licznie wzbudzać będą więcej elektronów, a te proporcjonalnie mocniej skalować będą efekt lawinowy wybijania kolejnych elektronów w silnie spolaryzowanym półprzewodnikowym złączu p-n jednofotonowej diody.

Stąd jednym z możliwych podejść do minimalizowania wpływu fluktuacji liczby fotonów w impulsie laserowym jest stosowania zaawansowanych metod optyki kwantowej, np. w zakresie generacji fundamentalnie pojedynczych fotonowych stanów splątanych, w których tylko jeden foton występuje w danym stanie kwantowym, np. o określonej polaryzacji (co jest weryfikowane statystycznie w wielu zdarzeniach elementarnych poprzez monitorowanie złamania nierówności Bella/CHSH na klasyczne limity lokalnych korelacji pomiarowych odpowiadające zachowaniu związków przyczynowo-skutkowych).

Jest to kolejnym powodem, dla którego badania empiryczne procesu fotoelektrycznego jako źródła losowości powinny być rozszerzone i realizowane łącznie w zakresie bardziej zaawansowanej optyki kwantowej (tj. również w domenie przestrzennej a nie tylko czasowej, i także w zakresie nielokalnego splątania kwantowego zaburzającego zasadę lokalności i związki przyczynowo-skutkowe), co też opisano w kolejnych paragrafach.

Kwantowa generacja losowości w oparciu o nanoplazmoniczne wzmocnienie efektu fotoelektrycznego (w ramach zjawisk kwantowej nano-plazmoniki w domieszkowanych nano-metalicznie nanocząstkami półprzewodnikach przy wykorzystaniu pośrednictwa plazmonów w efekcie fotoelektrycznym)

Pogłębiona analiza teoretyczna zjawisk kwantowych w dynamice nano-plazmonicznej opisana jest w autorskiej publikacji P-15 pozostającej w związku z przedmiotowym wycinkiem badań w ramach etapu nr 2 projektu. Analiza efektów kwantowych w ramach oryginalnie rozwiniętej teorii przybliżenia faz chaotycznych dla układów metalicznych nano-cząstkek, w których drgania cieczy elektronowej nazywane są plazmonami, wykazała, że ich skala w stosunku do energii dynamiki plazmonów jest na tyle niewielka (np. efektu spill-out, tj. kwantowego wylewania się cieczy elektronowej poza cząstkę), że minimalizuje możliwości ich praktycznego wykorzystania do generacji losowości w samych metalicznych nanocząstkach (tj. w czysto plazmonowych układach).

Pomimo, że w zintegrowanych układach potencjalnie opartych na domieszkowanych metalicznie nano-cząstkami diodach półprzewodnikowych wykazujących silne plazmonowe wzmocnienie zjawiska fotoelektrycznego w absorpcji fotonów padających na półprzewodnik sytuacja jest bardziej korzystna (ten plazmonowy efekt jest kwantowy i łatwo mierzalny), to jednak uwarunkowania tego procesu nie pozwalają na implementację praktycznego źródła generacji liczb losowych (największym problemem jest tu wzbudzanie plazmonu w nanocząstce w sposób kwantowy, gdyż energia plazmonu, tj. kolektywnego drgania cieczy elektronowej nie odpowiada skali energetycznej pojedynczych fotonów padających na plazmonicznie modyfikowaną fotodiodę, będących uwarunkowaniem kwantowej losowości źródła modelowanej statystyką według rozkładu Poissona). Z tego też powodu mechanizm fizyczny nano-plazmonicznego wzmocnienia efektu fotoelektrycznego dla generacji losowości kwantowej nie został określony jako najoptymalniejszy dla wykorzystania w

generatorze QRNG. Szczegóły dotyczące zjawisk kwantowych i ich skal w nano-plazmonice znajdują się w ww. publikacji P-15 (jest to pozostająca w związku z badaniami projektowymi publikacja w języku angielskim w postaci monografii „Quantum Nano-Plasmonics" wydana w 2020 r. przez Cambridge University Press, w której członek zespołu badawczego projektu – W. Jacak – analizuje efekty kwantowe w nano-plazmonice w oryginalnie rozwiniętej teorii RPA w nano-cząstkach metalicznych także sprzężonych z półprzewodnikiem).

Szczegóły dotyczące zjawisk kwantowych i ich skal w nano-plazmonice znajdują się w ww. publikacji P-15 (jest to pozostająca w związku z badaniami projektowymi publikacja w postaci monografii „Quantum Nano-Plasmonics" wydana w 2020 r. przez Cambridge University Press, w której członek zespołu badawczego projektu – W. Jacak – analizuje efekty kwantowe w nano-plazmonice w oryginalnie rozwiniętej teorii RPA w nano-cząstkach metalicznych także sprzężonych z półprzewodnikiem).

Kwantowa generacja losowości w oparciu o układy optyki kwantowej

Generacja losowości w zakresie układów optyki kwantowej może wykraczać poza domene czasową charakterystyczną dla układów opartych o efekt fotoelektryczny w detektorze jednofotonowym (lub ogólniej w układach półprzewodnikowych). W celu włączeniu niedeterminizmu przestrzennego jako źródła losowości należy zapewnić, że fotony w sposób niedeterministyczny będą poruszać się po różnych drogach optycznych w układzie optyki kwantowej.

Podstawowym sposobem realizacji takiej koncepcji jest rozdzielanie wiązki fotonowej, np. za pomocą półprzepuszczalnych zwierciadeł. W najprostszym modelowym ujęciu pojedyncze fotony podróżujące przez układ typu półprzezroczystego zwierciadła, pod warunkiem, że jest ono rzeczywiście idealnie półprzepuszczalne, mają prawdopodobieństwo dokładnie równe 50% odbicia lub transmisji przez takie zwierciadło (konfiguracja półprzepuszczalnego zwierciadła, implementowanego zwykle przez tzw. rozdzielacz wiązki, jest najczęściej taka, że fotony transmitowane poruszają się za zwierciadłem w równoległej trajektorii optycznej z trajektorią padania, a odbite są skierowane w trajektorii pod kątem prostym (zwierciadło półprzepuszczalne jest ustawione pod kątem 45 stopni, co efektywnie ma miejsce w implementacji tzw. kostki światłodzielącej czy rozdzielaczu wiązki).

Najczęstszą konstrukcją tego powszechnego elementu optycznego jest forma szklanego sześcianu, na którą składają się 2 przestrzennie trójkątne szklane pryzmaty, które są sklejone ze sobą u podstawy (najczęściej za pomocą klejów poliestrowych, epoksydowych lub uretanowych). Grubość i rodzaj warstwy kleju jest dobierana tak, aby dla jedynie pewnej długości fali połowa światła padająca na powierzchnię kostki światłodzielącej była odbijana, a druga połowa transmitowana w efekcie udaremnionego całkowitego odbicia wewnętrznego (frustrated total internal reflection, FTIR). Ponadto polaryzacyjne rozdzielacze wiązki, takie jak np. pryzmat Wollastona, wykorzystują materiały

optyczne silnie dwójłomne do dzielenia światła na dwie wiązki o ortogonalnych względem siebie stanach polaryzacji.

Dwa wzajemnie wykluczające się (klasycznie) zdarzenia (odbicie oraz transmisja) są wykrywane przestrzennie na końcach 2 dróg optycznych (co najmniej 2 detektorami fotonów) i kodowane odpowiednio wartościami bitowymi 0 lub 1 z prawdziwie losowym rozkładem w generowanym ciągu binarnym w efekcie serii ww. przejść przez rozdzielacz wiązki, przy uwarunkowaniu jednak dynamiką kwantową (tj. jedynie w sytuacji, w której na różnych przestrzennie drogach optycznych poruszają się pojedyncze fotony, które przed pomiarem podlegają pełnemu niedeterminizmowi, tj. nieokreśloności lub inaczej superpozycji jednoczesnego występowania na obu dostępnych im drogach optycznych, dopóki nie zostanie wykonany pomiar, powodujący w pełni losowe rzutowanie von Neumanna, tj. kolaps superpozycji dróg optycznych i klasyczne ustalenie którą drogą optyczną podróżował foton poprzez zarejestrowanie tego fotonu w określonym jednym z 2 detektorów, przypisanych do właściwej drogi optycznej w układzie).

Problematyka uzyskania pojedynczych stanów kwantowych (fotonów) warunkujących dynamikę kwantową w układzie optycznym jest złożonym problemem omawianym w poprzednich paragrafach. Jednym z fundamentalnych rozwiązań tego problemu jest wykorzystanie splątania kwantowego w stanach polaryzacji fotonów (np. w zakresie techniki spontanicznej parametrycznej konwersja w dół typu II prowadzącej do wyboru binarnego stanu fazy w zdegenerowanym optycznym oscylatorze parametrycznym).

Spontaniczna parametryczna konwersja w dół, SPDC (często nazywana też fluorescencją parametryczną lub rozpraszaniem parametrycznym) to nieliniowy proces optyczny, w którym pojedynczy foton o dużej energii – tzw. foton pompujący (pump) – ulega konwersji w dwa fotony o niższej energii (tzw. konwersja w dół), tj. tzw. foton sygnałowy (signal) oraz foton uboczny (idler). Proces ten przebiega w pełni w zgodzie z zasadą zachowania energii i pędu (dwa fotony powstałe w wyniku procesu mają sumaryczną energie i pędy równe energii i pędowi fotonu wejściowego oraz fononów w sieci krystalicznej, które biorą udział w procesie w obrębie kryształu).

Ponieważ współczynnik załamania zmienia się wraz z częstotliwością (efekt dyspersji), tylko niektóre tryplety częstotliwości 3 fotonów biorących udział w procesie SPDC będą dopasowywane fazowo tak, aby można było uzyskać równoczesne spełnienie zasady zachowania energii oraz zasady zachowania pędu. Właściwe dopasowanie fazowe najczęściej uzyskuje się przy użyciu silnie dwójłomnych materiałów nieliniowych, których współczynnik załamania zmienia się wraz z polaryzacją. Z tego też powodu podstawowe typy spontanicznej parametrycznej konwersji w dół wprowadza się na podstawie wzajemnych relacji polaryzacji trójki fotonów - wejściowego fotonu pompującego (pump) oraz 2 fotonów wyjściowych (signal i idler).

Spontaniczna parametryczna konwersja w dół typu 0 zachodzi gdy wszystkie 3 fotony mają taką samą polaryzację. W przypadku gdy fotony wyjściowe (signal i idler) mają taką samą polaryzację, jednak

prostopadłą do fotonu wejściowego (pump) zachodzi spontaniczna parametryczna konwersja w dół typu I. Jeśli zaś fotony wyjściowe (signal i idler) mają polaryzację wzajemnie prostopadłą zachodzi spontaniczna parametryczna konwersja w dół typu II. Wydajność konwersji fotonów w procesie spontanicznej parametrycznej konwersji w dół jest zwykle bardzo niska.

Możliwie wysokie parametry uzyskuje się w tzw. przekładańcach periodycznie spolaryzowanych silnie dwójłomnych ośrodków optycznych (przykładowy rezultat o relatywnie wysokiej efektywności to jedynie 4 pary fotonów wyjściowych na aż 10^6 fotonów wejściowych w periodycznie spolaryzowanym niobianie litu - *periodically-poled lithium niobate* PPLN).

O ile jednak pojedynczy foton (stanowiący połówkę pary) – tj. foton sygnałowy (signal) – zostanie wykryty, istnieje wówczas pewność, że sparowany z nim foton uboczny (idler) również został wygenerowany w tym procesie (dzięki temu proces SPDC jest dobrym źródłem obiektywnie weryfikowalnym pomiarem fotonu sygnałowego pojedynczych fotonów ubocznych związanych z sygnałowymi w parach).

Procesy SPDC są jednymi z bardziej zaawansowanych procesów optyki kwantowej. W najczęstszej konfiguracji takich układów proces SPDC inicjuje silna wiązka laserowa (tzw. wiązka pompukąca) kierowana na także silnie dwójłomny nieliniowy optycznie kryształ, np. beta-boranu baru (BBO). niobianu litu (LN) lub dwuwodorofosforanu potasu (KDP). Ogromna większość fotonów przechodzi przez taki kryształ niezmieniona, jednak czasami (raz na milion lub więcej fotonów) niektóre fotony spontanicznie ulegają procesowi spontanicznej parametrycznej konwersji w dół typu II, w której powstałe dwa fotony są wzajemnie prostopadłe a ich trajektorie są ograniczone krawędziami dwóch stożków optycznych wychodzących z kryształu, których osie ustawiają się symetrycznie względem wchodzącej wiązki pompującej.

Mający miejsce proces ma nieliniowy charakter w sensie optycznym (elektromagnetycznym), jednak podlega opisowi kwantowo mechanicznemu (w kategoriach fotonicznej absorpcji i emisji w krzysztale, z uwzględnieniem oddziaływania z siecią krystaliczną – tj. z fononami).

Z powodu obowiązującej zasady zachowania pędu, dwa wygenerowane (emitowane) w takim procesie fotony są zawsze symetrycznie zlokalizowane przestrzennie względem wiązki pompującej, co pozwala na ich separację w oddzielnych drogach optycznych za pomocą odpowiednio skalibrowanego przestrzennie układu optyki kwantowej.

Trajektorie pary fotonów mogą przebiegać dwoma liniami znajdującymi się w obszarze przecinania się krawędzi obu stożków, co skutkuje splątaniem polaryzacyjnym pary fotonów (są one spolaryzowane prostopadle względem siebie). Inicjowanie procesu SPDC typu I (w którym fotony wyjściowe mają taką samą polaryzację) jest najczęściej realizowane z wykorzystaniem kryształu dwuwodorofosforanu potasu (KDP), w odróżnieniu do procesów SPDC typu II, które zachodzą w kryształach beta-boranu baru (BBO).

Procesy SPDC typu II generujące splątania kwantowego fotonów w ich polaryzacyjnych stopniach swobody (splątanie w postaci antysymetrycznych stanów Bella dla polaryzacji fotonów, tj. przeciwne polaryzacje dola obu wyjściowych fotonów) w kryształach BBO są zjawiskiem czysto kwantowym, a korelacje splątaniowe wyników polaryzacji fotonów stanowią potencjalne, wysokiej jakości kwantowe źródło losowe, zapewniające pojedyczne fotony (pomiar fotonu sygnałowego determinuje obecność tylko pojedynczego fotonu ubocznego w pełni antysymetrycznym stanie polaryzacji).

Badanie w zakresie wykorzystania optyki kwantowej do generacji prawdziwej losowości oparte są o własny układ modułu optycznego Seqre Crystal, obejmujący układ generacji splątania kwantowego w procesie SPDC typu II na krysztale BBO, rozwijany we współpracy międzynarodowej przez zespół badawczy realizatora projektu od 2012 roku.

Układ ten wykorzystuje polaryzację fotonów i polaryzujące kostki światłodzielące (*polarizing beam splitters*) przy jednoczesnym wprowadzeniu splątania kwantowego w procesie spontanicznej parametrycznej konwersji w dół typu II dla zapewnienia jednofotonowych stanów kwantowych w stopniach swobody polaryzacji i możliwości niezależnej weryfikacji kwantowości źródła przez empiryczne wykazanie złamania nierówności Bella (układ ten rozwijany jest przez zespół projektowy w kontynuacji wcześniejszych projektów badawczych ukierunkowanych na kryptografię kwantową).

Szczegóły analizy układów optyki kwantowej w ujęciu niedeterminizmu przestrzennego zawarto w publikacji P-4.

Kwantowa generacja losowości w oparciu o rozpady promieniotwórcze

Źródło promieniowania rozpadu jądrowego ma absolutnie losowy (kwantowy) charakter dynamiki. Może być wykrywane przez licznik Geigera-Mullera podłączony do dedykowanego układu elektronicznego lub komputera.

W zjawisku rozpadu promieniotwórczego źródłem losowości są kwanty promieniowania jonizującego wykrywane przez detektory typu Geigera-Mullera, miniaturowe gazowe lub ciałostałowe komory jonizacyjne, efektywniejsze detektory półprzewodnikowe (oparte na krzemie lub germanie) albo bardziej zaawansowane detektory scyntylacyjne. Odpowiednia konfiguracja detektorów jonizacji charakteryzuje się wysoką efektywnością pomiarów niedeterministycznych procesów kwantowych, jednak skale energetyczne tych procesów są oczywiście bardzo wysokie, co przekłada się także na trwałość detektorów i stwarza problemy z ich miniaturyzacją przy zachowaniu wysokiego poziomu trwałości elementów detekcyjnych umożliwiającego generowanie losowych ciągów binarnych przy zapewnieniu wysokiej częstotliwości tej generacji przez dłuższe okresy funkcjonowania układu.

Zaletami wykorzystania w procesach QRNG układów opartych na rozpadzie jądrowym jest ich prostota implementacyjna (wystarczy niewielka ilość nawet nisko radioaktywnego materiału, który

dokonując rozpadu promieniotwórczego zagwarantuje rozkład prawdziwie losowy, modelowany rozkładem Poissiona, odpowiedniego do procesu, w którym znana jest średnia wartość zdarzeń elementarnych w przedziale czasowym, ale zajście poszczególnego zdarzenia elementarnego pozostaje całkowicie niezależne od czasu dzielącego to zdarzenie od poprzedniego takiego zdarzenia.

Zasadniczą jednak wadą wykorzystania procesów promieniotwórczych dla bezpiecznej generacji losowości jest wysokoenergetyczność kwantów promieniowania w procesach rozpadu jądrowego.

W efekcie lawiny Townsenda (G-M) w polu elektrycznym (samosprzężone zwielokrotnienie lawinowe jonizacji wzmocnionej przez emisję fotonów UV) następuje wzbudzenie od 10^9 do 10^{10} par jonowych z pojedynczego zjawiska jonizującego, co zwielokrotnia szum kwantowy pierwotnie o niskiej mocy do relatywnie wysokiej, wówczas bardzo łatwy do zarejestrowania.

W problematyce wysokich energii kwantów promieniowania rozpadu jądrowego nie chodzi jedynie o trwałość elementów detekcyjnych w warunkach ciągłej pracy przy generacji losowych ciągów binarnych z wysokimi częstotliwościami, ale zasadniczo znacznie bardziej o możliwość wykrycia zewnętrznej sygnatury fizycznej konsekwencji zdarzenia elementarnego (wysoka energia kwantu promieniowania powoduje całą kaskadę wzbudzenia na tyle silnego energetycznie, że ryzykowna staję się możliwość jego wykrycia na zewnątrz układu generatora).

Chodzi tu zatem o wyciek informacji dotyczących poszczególnych zdarzeń elementarnych z układu generatora opartego o procesy promieniotwórcze, stwarzający możliwość podsłuchu nawet zewnętrzną obserwacją generatora (ułatwia to dodatkowo charakterystyka działania detektora, który po wyzwoleniu lawiny kwantem przez pewien krótki okres podlega refrakcji nie rejestrując w tym okresie kolejnych zliczeń mimo padania na detektor kolejnych kwantów promieniowania – tzw. czas martwy detektora). Dalsze szczegóły zawarto w publikacji P-4.

Podsumowanie

W toku badań projektowych w ramach etapu nr 2 projektu określono jako optymalne, wydajne i przy tym zupełnie bezpieczne dla użytkownika koncepcje bezwarunkowego źródła entropii w schemacie przejść kwantowych zgodnie ze złotą regułą Fermiego w praktycznym wykorzystaniu takich przejść w przyrządach elektronicznych (w zakresie źródeł losowości opartych o szum śrutowy). Szczegółowa analiza uzasadniająca taki wybór znajduje się w publikacji P-4, zaś szczegółowe wyniki badania w zakresie testów statystycznych kwantowo generowanej losowości przedstawiono w publikacji P-5.

Po zakończeniu realizacji etapu 2 projektu rozpoczęto trwające obecnie i zaawansowane już prace w zakresie realizacji etapu 3, tj. w zakresie prototypowania układu QRNG.

Główne osiągnięcie w kontynuacji prac badawczych w ramach prototypowania układu generacji kwantowej losowości QRNG dotyczą jego postępującej miniaturyzacji. Obecnie prowadzone są prace

badawcze ukierunkowane na integrację prototypu do rozmiarów bardzo małego układu scalonego możliwego do zainstalowania w dowolnie małym komputerze, a nawet telefonie komórkowym – rozmiary rzędu (1 x 0,5 x 2 cm) lub mniejsze.

Dotychczasowe wyniki badawcze osiągnięte w ramach realizacji projektu zostały opublikowane w dwóch publikacjach w czasopiśmie naukowym Scientific Reports wydawnictwa Nature Springer w 2020 (publiakcja P-8 – publikacja uzykała 5-te miejsce w kolekcji 'Top 100 in Physics' w 2020 roku w czasopiśmie Scientific Reports (Nature Springer) [https://www.nature.com/collections/ihggebhehd]) i 2021 (publikacja P-9), z wysokim wskaźnikiem Impact Factor wynoszącym 4,8 – publikacje dostępne są też pod adresami internetowymi https://www.nature.com/articles/s41598-019-56706-2 oraz https://www.nature.com/articles/s41598-021-95388-7), a jakość i zasięg tego czasopisma podkreśla istotne osiągnięcie naukowo-techniczne w skali międzynarodowej odnośnie weryfikacji losowości generowanego ciągu losowego i analiz dotyczących wyboru optymalnego źródła losowości kwantowej.

Ważnym aspektem dotychczasowych osiągnięć projektu (które po raz pierwszy zostało upublicznione w międzynarodowym zgłoszeniu patentowym PCT zespołu projektowego już w grudniu 2017 roku) jest silne jego podobieństwo do głośnego sukcesu firmy Google z października 2019 r. powszechnie uznawanego za przełom w zakresie informatyki kwantowej, tj. osiągnięcia tzw. przewagi kwantowej w zakresie przedstawienia architektury oraz implementacji 53-qubitowego procesora komputera kwantowego Google Sycamore, działającego i osiągającego przewagę kwantową właśnie w obszarze weryfikacji losowości rozkładu ciągu binarnego (tj. bezpośrednio w tematyce przedmiotowego projektu), co zespół badawczy wykazał w patencie z grudnia 2017 r. (wynikającym z realizacji projektu), a więc na około 2 lata przed publikacją ujawniającą późniejszą specyfikację układu Google i rezultatu osiągnięcia tzw. kwantowej przewagi.

W odniesieniu do istotnych pośrednich rezultatów realizacji projektu, należy podkreślić, że opracowane koncepcje techniczne weryfikacji losowości kwantowej zostały przyjęte w 2020 r. przez ponad 150 osobowy komitet ekspercki Kwantowej Grupy Standaryzacyjnej w sekcji Kwantowej Generacji Losowości Europejskiego Instytutu Certyfikacji Informatycznej w Brukseli jako zestaw trzech standardów referencyjnych dla kwantowej generacji losowości w podobnej koncepcji (jednak opisanej 2 lata wcześniej), którą wykorzystuje architektura procesora kwantowego Google Sycamore (więcej informacji pod adresem https://eitci.org/technology-certification/qsg/eqrng).

Włączenie dotychczasowych wyników realizacji projektu jako podstawy dla europejskich standardów referencyjnych dla nowych technologii informacyjno-komunikacyjnych w obszarze kwantowym (wspierających obecnie dynamicznie rozwijaną inicjatywę Quantum Flagship Komisji Europejskiej, zakładającej finansowanie badań w obszarze technologii kwantowej w intensywności co najmniej 1 miliarda euro) stanowiło część aktywności standaryzacyjnej zespołu projektowego w programie StandICT Horizon 2020.

Międzynarodowy charakter uznania istotności osiągnięć w zakresie otrzymanych dotychczas wyników badawczych projektu POIR.01.01.01-00-0173/15, a także aktualności problematyki przedmiotowego zagadnienia (przede wszystkim wobec przełomu technologicznego tzw. przewagi kwantowej Google z października 2019 r. i dużej zbieżności architektury układu Google jak i rozwiązywanego problemu w zakresie weryfikacji losowości rozkładu binarnego z układem opatentowanym przez realizatora projektu 2 lata wcześniej, jak również powtórzenia rezultatu osiągnięcia przewagi kwantowej w USTC w Hefei z 2020 r. w Chinach), jest znaczącym sukcesem dotychczasowej realizacji projektu.

Należy również dodać, że bieżącymi wynikami realizacji projektu interesuje się Departament Innowacji i Rozwoju Ministerstwa Nauki i Szkolnictwa Wyższego (obecnie Ministerstwa Edukacji i Nauki), który z własnej inicjatywy wysyłał kilkukrotnie zapytania do koordynatora projektu (ostatnie z listopada 2020 roku) o postęp w pracach i możliwości wsparcia krajowego wkładu w europejski program nowej kwantowej infrastruktury komunikacyjnej (inicjatywa EuroQCI - European Quantum Communication Infrastructure, w którą włączyły się wszystkie państwa członkowskie UE). Zespół projektu jest zainteresowany wspieraniem rozwoju krajowej jak również europejskiej infrastruktury komunikacji kwantowej i pozostaje w związku z tym w komunikacji i współpracy z DIiR MNiSW (obecnie MEiN).

W tym zakresie zespół projektowy uczestniczy aktywnie w konsultacjach dziedzinowych zainicjowanych przez DIiR, a także Centrum Kwantowych Technologii Optycznych Uniwersytetu Warszawskiego (https://www.uw.edu.pl/centrum-kwantowych-technologii-optycznych), oraz Polskiej Platformy Technologicznej Fotoniki (http://www.pptf.pl/konsorcjanci), w tym w konsultacjach dot. europejskich i krajowych kwantowych łączy satelitarnych. Ważnym zagranicznym współpracownikiem naukowym zespołu jest jeden z głównych ekspertów AIT dr Andreas Poppe, współpracownik prof. Antona Zeilingera związanego z implementacją chińskiej demonstracji komunikacji kwantowej w przestrzeni kosmicznej w 2015 r. – satelita Micius w programie QUESS; Dr Andreas Poppe kieruje obecnie programem komercyjnym kryptografii kwantowej w europejskim centrum badawczym w Monachium, a z zespołem projektowym realizował w przeszłości wiele innych projektów powiązanych dziedzinowo w zakresie kryptografii kwantowej.

Jako, że w działaniu układów kryptografii kwantowej (QKD) o ważnym znaczeniu strategicznym w dziedzinie cyberbezpieczeństwa krytyczną rolę odgrywają komponenty kwantowej generacji losowości QRNG, które dla zachowania bezpieczeństwa nie mogą być dostarczane przez zagranicznych dostawców, prace w projekcie implementacji krajowych generatorów losowości kwantowej są kluczowym elementem w pełni krajowych układów QKD niezależnie od ich typów, m.in. np. implementacji w zakresie kwantowych zmiennych ciągłych – jednego z perspektywicznych obszarów rozwoju kwantowej kryptografii oraz przyszłościowego kwantowego Internetu.

Realizacja krajowych układów QKD (bez zagranicznych komponentów układów mogących wprowadzać tzw. ‘tylne drzwi’ do urządzeń pozornie bezwarunkowo bezpiecznych) jest niemożliwa

bez wytworzenia w pełni krajowych układów kwantowej generacji losowości, co też pozostaje głównym celem projektu i jest obecnie w fazie prototypowej.

Szczegółowy opis wyników technologicznych zespołu badawczego projektu w dziedzinie badań i rozwoju krajowych układów kwantowej generacji losowości QRNG i kwantowej dystrybucji klucza QKD (w zakresie kryptografii kwantowej) znajduje się na stronie https://seqre.net/commercialization.

Według specjalistycznej wiedzy zespołu projektowego o ekspertyzie naukowo-technicznej w dziedzinie realizacji projektu prace badawczo-rozwojowe ukierunkowane na komercjalizację kryptografii kwantowej w skali międzynarodowej są znacząco wspierane polskimi wysiłkami oraz rezultatami w strategicznej dziedzinie bezpieczeństwa informatycznego osiąganymi z szerszym uznaniem i zgodnie z planem projektowym przez krajowego realizatora projektu stanowiącego element rozwoju krajowej kryptografii kwantowej bez komponentów od zagranicznych dostawców, co jest również kluczowe w dziedzinie o strategicznym znaczeniu dla bezpieczeństwa narodowego.

Krytycznym aspektem programu komercjalizacji kryptografii kwantowej o istotnym znaczeniu dla bezpieczeństwa narodowego w zakresie cyberbezpieczeństwa są prace badawcze prowadzone w niniejszym projekcie nad krytycznymi dla funkcjonowania kryptografii kwantowej układami kwantowej generacji losowości QRNG (przedmiotowe badania projektowe zostały potwierdzone decyzją NCBiR z 2021 roku jako mające charakter badań dotyczących strategicznego bezpieczeństwa narodowego, wyszczególnionych w odnośnych przepisach).