SZCZEGÓŁOWY OPIS ZREALIZOWANYCH PRAC BADAWCZYCH ORAZ UZYSKANYCH WYNIKÓW W RAMACH ETAPU 2 PROJEKTU PT. ”JURAND – NARODOWY KWANTOWY GENERATOR LICZB LOSOWYCH”

Niniejszy dokument zawiera podsumowanie wyników prac badawczych zrealizowanych w ramach etapu nr 2 projektu „JURAND – Narodowy Kwantowy Generator Liczb Losowych”, podlegając 10-stronicowemu limitowi w zawartości dokumentu według specyfikacji Narodowego Centrum Badań i Rozwoju.

Właściwe rozwinięcie niniejszego podsumowania znajduje się w dokumencie „R-2: Raport z realizacji badań przemysłowych w ramach etapu nr 2 projektu”, stanowiącym kamień milowy z realizacji etapu nr 2 projektu – dostępnym pod adresem:

https://seqre.net/sites/default/files/resources/generic/jurand/R-2-raport2.pdf

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 projektu) 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
  https://seqre.net/sites/default/files/resources/generic/jurand/R-2-raport2.pdf
- 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).

Pełna analiza wyników badawczych w kierunku określenia optymalnego procesu kwantowego dla generacji losowości w zintegrowanym i praktycznym układzie QRNG znajduje się w publikacji P-4 oraz w szeregu pozostałych publikacji specjalistycznych i zbiorów danych źródłowych wskazanych powyżej

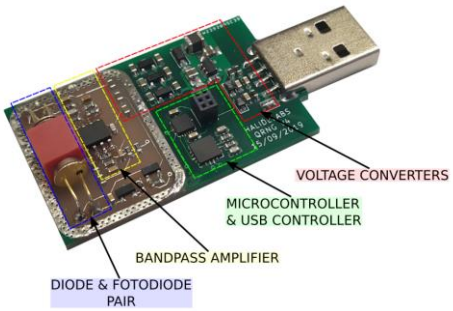
i stanowiących wyniki realizacji etapu nr 2 projektu, a także w rozwiniętym opisie sprawozdawczym z realizacji tego etapu projektu w raporcie R-2 (stanowiącym kamień milowy realizacji projektu).

W toku badań projektowych w ramach etapu nr 2 projektu określono jako optymalne, wydajne i przy tym zupełnie bezpieczne dla użytkownika koncepcje prawdziwie niedeterministycznego 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 nr 2 projektu rozpoczęto trwające obecnie i zaawansowane już prace w zakresie realizacji etapu nr 3, tj. w zakresie prototypowania układu QRNG.

Rys.1. Zdjęcia poglądowe prototypowego układu kwantowego generatora liczb losowych wytworzonego według własnej specyfikacji w oparciu o zjawisko kwantowego szumu śrutowego w toku realizacji projektu JURAND

Główne osiągnięcia w kontynuacji prac badawczych w ramach prototypowania układu generacji kwantowej losowości QRNG w etapie nr 3 dotyczą jego postępującej miniaturyzacji względem poprzednich iteracji. 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.



Rys.2. Zdjęcia poglądowe w zakresie dalszej miniaturyzacji prototypowego układu kwantowego generatora liczb losowych wytworzonego według własnej specyfikacji w oparciu o zjawisko kwantowego szumu śrutowego w toku realizacji etapu nr 3 projektu JURAND ze wskazaniem kluczowym bloków funkcjonalnych tego układu

Dotychczasowe wyniki badawcze osiągnięte w ramach realizacji projektu po zakończeniu etapu nr 2 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 następującymi adresami internetowymi wydawnictwa Nature Springer: 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 istotność osiągnięcia naukowo-technicznego 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), jak również 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.

Zasadniczym 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).

Z uwagi na limit objętości niniejszego dokumentu w specyfikacji NCBiR rozwinięcie podsumowania wyników z realizacji prac badawczych etapu nr 2 projektu znajduje się w dokumencie „R-2: Raport z realizacji badań przemysłowych w ramach etapu nr 2 projektu” – dostępnym pod adresem:

https://seqre.net/sites/default/files/resources/generic/jurand/R-2-raport2.pdf.