Załącznik 1. Wyniki prac badawczych podlegających komercjalizacji i ochronie patentowej

uzyskanych w toku realizacji projektu „Prace badawczo-rozwojowe w kierunku komercjalizacji kryptografii kwantowej w układach bezsplątaniowych i splątaniowych”

Projekt „Wsparcie procedur patentowych i ochrony praw własności przemysłowej w obszarze komercjalizacji kryptografii kwantowej” – CompSecur sp. z o.o.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

Spis treści

Podsumowanie menadżerskie 3
1. Wstęp 6
2. Geneza projektu 7
3. Cel główny projektu 12
4. Opis przeprowadzonych badań przemysłowych 12
5. Opis przeprowadzonych prac rozwojowych 23
6. Wyniki z przeprowadzonych badań przemysłowych i prac rozwojowych – uzasadnienie osiągnięcia założeń zawartych we wniosku i biznesplanie 26
7. Analiza SWOT I Etapu projektu (Mocne strony, Słabe strony, Szanse, Zagrożenia) 26
Mocne strony 27
Słabe strony 28
Szanse 29
Zagrożenia 29
8. Ocena krytyczna wyników prac badawczych projektu 30
9. Wnioski płynące z realizacji I Etapu projektu 35
10. Szczegółowe wyniki prac badawczych 39

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

Podsumowanie menadżerskie

Kryptografia kwantowa lub kwantowa dystrybucja klucza (ang. quantum key distribution QKD) stanowi jedyne pewne zabezpieczenie tajnej komunikacji zdalnej przed ewentualnym atakiem na szyfry z wykorzystaniem komputera kwantowego nad konstrukcją którego trwają zaawansowane już prace, oferując równocześnie po raz pierwszy w historii teoretycznie bezwarunkowy poziom bezpieczeństwa komunikacji, możliwy do wdrożenia w obecnie stosowanych infrastrukturach telekomunikacyjnych. Podczas gdy komputery kwantowe stają się rzeczywistością (w maju 2013 roku NASA i Google we wspólnym przedsięwzięciu wdrożyły 512 qubitowe nadprzewodzące komputery kwantowe DWave Two, tworząc pierwsze na świecie kwantowe laboratorium sztucznej inteligencji) bezpieczeństwo krytycznej, tajnej komunikacji podlega procesowi przewartościowania. Klasyczne kryptosystemy, opierające się na matematycznych problemach trudnych zostały zakwestionowane, jako że problemy te mogą być skutecznie rozwiązane przez komputery kwantowe, w badaniach nad którymi osiąganych jest coraz więcej przełomów technologicznych. Z nadchodzącą rewolucją informatyki kwantowej wiąże się coraz szerzej dostrzegane zagrożenie dla rozmaitych zabezpieczeń komunikacji o kluczowej roli dla instytucji sektora finansów i bankowości, a także w wymiarze pozakomercyjnym o charakterze bezpieczeństwa narodowego dla administracji publicznej i wojska.

W toku realizacji projektu „Prace badawczo-rozwojowe w kierunku komercjalizacji kryptografii kwantowej w układach bezsplątaniowych i splątaniowych" w ramach przeprowadzonych badań rozpoznano możliwości oraz uwarunkowania techniczne dla przygotowania do wdrożenia i komercjalizacji układów kryptografii kwantowej wykorzystującej protokoły zarówno nieoparte jak i oparte na splątaniu kwantowym. Uwarunkowania techniczne obecnego stanu rozwoju optyki kwantowej dla celów zastosowań w rzeczywistych sieciowych środowiskach komercyjnych były testowane w toku badań przemysłowych i prac rozwojowych w warunkach laboratoryjnych. Badania zakończyły się osiągnięciem z sukcesem celów projektowych i zakładanych wskaźników projektowych (w tym z ich przekroczeniem). W szczególności zrealizowane badania pozwoliły przeprowadzić pilotażowe wdrożenia obu rodzajów prototypowych układów QKD (bezsplątaniowych i splątaniowych) w metropolitalnej sieci światłowodowej we Wrocławiu. W toku realizacji projektu dokonano eksperymentalnego wdrożenia we Wrocławiu jednej z pierwszych na świecie prototypowych metropolitalnych sieci kwantowych QKD łączących splątaniową i bezsplątaniową komunikację kwantową (w czasie prowadzenia eksperymentalnych wdrożeń metropolitalnych w miejskiej infrastrukturze światłowodowej w latach 2013 i 2014 hybrydowe sieci QKD łączące układy splątaniowe i bezsplątaniowe były eksperymentalnie wdrażane poza Wrocławiem tylko w Wiedniu i w Tokio – co uczyniło z Wrocławia trzecie miasto na świecie, które dysponowało taką siecią w szkieletowej infrastrukturze telekomunikacyjnej).

Szczegółowe wyniki badań i prac rozwojowych w projekcie zostały upowszechnione w formie publikacji w międzynarodowych czasopismach specjalistycznych, oraz w formie prezentacji na międzynarodowych konferencjach w dziedzinie kryptografii kwantowej. W szczególności wyniki projektu prezentowano na następujących międzynarodowych konferencjach:

- 2nd Annual International Conference on Quantum Cryptography QCrypt 2012,
  10 – 14 wrzesień 2012, Singapur

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

- 3rd Annual International Conference on Quantum Cryptography QCrypt 2013, 5 – 9 sierpień 2013, Waterloo, Kanada
- 1st Quantum Cryptography Standardization Symposium - Quantum-Safe-Crypto Workshop, 26 – 27 wrzesień 2013, ETSI headquarters, Sophia Antipolis, Francja
- 5th LFPPI Symposium on Progress in Quantum Cryptography - seQre2014, 27 - 28 styczeń 2014, Wrocław, Polska
- 4th International Conference on Advanced Communications and Computation - INFOCOMP 2014, 20 – 24 lipiec 2014, Paryż, Francja, **gdzie prezentowanym wynikom badawczym przyznano nagrodę za najlepszą pracę naukową przedstawioną na konferencji.**

Ponadto, zgodnie z deklaracjami w projekcie, szczegółowe wyniki realizacji badań przemysłowych i prac rozwojowych zostały także zebrane i udostępnione na otwartej platformie internetowej http://www.seqre.net.

Część wyników projektu podlega obecnie procedurze zapewnienia ochrony własności intelektualnej w toku procedur patentowych przy wsparciu programu PatentPlus. Firma przygotowuje się równocześnie do kolejnego etapu wdrożeniowego polegającego na wprowadzeniu innowacyjnych, strategicznych i perspektywicznych produktów oraz usług opartych na wynikach badań przemysłowych i prac rozwojowych projektu do swojej oferty komercyjnej. W tym celu firma prowadzi działania w kierunku zapewnienia finansowania inwestycyjnego koniecznego do uruchomienia działań wdrożeniowych i produkcyjnych (prowadzone są rozmowy nt. inwestycji potrzebnych do wdrożenia linii produkcyjnych układów QKD z prywatnymi inwestorami i funduszami inwestycyjnymi typu Venture Capital oraz z instytucjami wsparcia inwestycyjnego, m.in. z Bankiem Gospodarstwa Krajowego, a także przygotowania do pozyskania funduszy inwestycyjnych w programie PO IR oraz w programie Bridge Venture Capital Narodowego Centrum Badań i Rozwoju). W dłuższej perspektywie komercjalizacja wyników badań projektowych zapewni wzrost przychodów i rentowności firmy w ramach wdrożeń komercyjnych planowanych w okresie trwałości projektu.

Poza wzrostem konkurencyjności oferty firmy realizatora projektu, istotnym rezultatem badań projektowych jest rozwój samej technologii kryptografii kwantowej, która ma duży potencjał dla unowocześnienia i zwiększenia konkurencyjności gospodarki krajowej względem gospodarek państw wysoko rozwiniętych, jak również strategiczne znaczenie dla bezpieczeństwa narodowego.

Osiągnięte w toku realizacji projektu wyniki prac badawczo-rozwojowych zostały przedstawione międzynarodowemu środowisku badawczemu w dziedzinie kryptografii kwantowej, a także komercyjno-rządowym sektorom potencjalnych odbiorców kryptografii kwantowej na specjalnie zorganizowanej w tym celu przez realizatora projektu międzynarodowej konferencji-sympozjum SEQRE 2014 (stanowiącej specjalną edycję w serii tradycyjnych sympozjów LFPPI na Politechnice Wrocławskiej) - http://www.seqre.net/seqre2014 - w dniach 27 i 28 stycznia 2014 roku.

Konferencja SEQRE 2014 prezentująca w międzynarodowym środowisku badawczym w tej dziedzinie wyniki realizacji projektu odbyła się pod honorowym patronatem Rektora Politechniki Wrocławskiej, Prezydenta Wrocławia oraz Dyrektora Narodowego Centrum Badań i Rozwoju. Skupiła ona najwybitniejszych światowych naukowców w dziedzinie kryptografii kwantowej, w tym twórców tej dziedziny, zaproszonych przez realizatora projektu i zespół naukowy odpowiedzialny za realizację badań. Poza prezentacją wyników badań zrealizowanych w projekcie, wykłady plenarne dotyczące światowych osiągnięć naukowych i technicznych w dziedzinie kryptografii kwantowej wygłosili m.in.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

prof. N. Gisin (Genewa), prof. A. Ekert (Oxford, Singapur), a także czołowi światowi technolodzy w tej dziedzinie: prof. V. Makarov (Waterloo), dr. A. Poppe (Wiedeń), dr. K. Tamaki (Tokio), dr. M. Lucamarini (Cambridge), dr. S. Kunz-Jacques (Paryż). Związane z problematyką kryptografii kwantowej krajowe teoretyczne badania podstawowe przedstawili prof. J. Rembieliński (Łódź) oraz prof. M. Czachor (Gdańsk). Przedstawiciele zespołu projektowego angażowanego przez realizatora projektu przedstawili szczegółowe wyniki badań przemysłowych i prac rozwojowych osiągniętych w projekcie do czasu organizacji konferencji oraz przeprowadzili szeroko zakrojone demonstracje technologiczne i specjalistyczne szkolenia w zakresie splątaniowej i bezsplątaniowej kryptografii kwantowej. O szczegółach innych światowych wdrożeń opowiedzieli przedstawiciele najważniejszych firm komercjalizujących kryptografię kwantową w innych krajach, w szczególności w Austrii, Szwajcarii, Francji, Wielkiej Brytanii oraz Japonii przedstawiając także demonstracje technologiczne.

W konferencji udział wzięli wysokiej rangi wojskowi przedstawiciele Ministerstwa Obrony Narodowej w ramach utworzonej w 2013r. struktury MON - Narodowego Centrum Kryptologii oceniający postęp w badaniach realizowanych w projekcie pod względem potencjału dla strategicznego bezpieczeństwa narodowego. Przedstawiciele MON/NCK zadeklarowali wysokie zainteresowanie technologią jako perspektywiczną dla bezpieczeństwa narodowego, niemającą klasycznych odpowiedników dla zapewnienia teoretycznie bezwarunkowego bezpieczeństwa tajnej komunikacji w zastosowaniach wojskowych. Reprezentowane były także banki zainteresowane komercyjnymi wdrożeniami tej technologii. Potencjalnym odbiorcom komercyjnym, również deklarującym zainteresowanie przyszłymi wdrożeniami przedstawiono szczegóły uzyskanych wyników projektowych w kontekście uwarunkowań wdrożeń w rzeczywistych środowiskach komercyjnych sieci metropolitalnych.

Wyniki badań oraz demonstracje technologiczne osiągnięte w projekcie zostały uznane przez komisję powołaną przez Prezydenta Wrocławia za jeden z „7 cudów Wrocławia", który zgodnie z deklaracją organizatorów będzie prezentowany w kategorii Nauka w ramach specjalnej wystawy z okazji obchodów dni Wrocławia jako Europejskiej Stolicy Kultury w 2016 roku.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

1. Wstęp

Kryptografia kwantowa, nad którą w ramach projektu prowadzono prace badawczo-rozwojowe w kierunku jej komercjalizacji, a ściślej tzw. kwantowa dystrybucja klucza (QKD, Quantum Key Distribution) jest zaawansowaną technologią kryptograficzną opartą na przetwarzaniu informacji kwantowej (QIP, Quantum Information Processing) – tj. nowoczesnej dziedzinie, której fundamenty teoretyczne obejmują fizykę kwantową oraz informatykę klasyczną. Wykorzystanie kwantowego układu (np. kwantowego stanu polaryzacji fotonu) jako nośnika informacji kwantowej (czyli fizycznego stanu układów kwantowych, podlegających całkowicie odmiennym od praw fizyki klasycznej, nieintuicyjnym prawom mechaniki kwantowej, które w szczególności obejmują nieoznaczoność i niedeterministyczny wynik pomiaru oraz naruszenie założenia lokalnego-realizmu) prowadzi do licznych przewag nad klasycznym odpowiednikiem nośnika informacji (klasycznym układom fizycznym) obecnie używanym w informatyce. Najważniejszą właściwością technologii kryptografii kwantowej jest osiągnięta dzięki niej po raz pierwszy w historii gwarancja zapewnienia teoretycznie bezwarunkowego (absolutnego, opartego na podstawowych prawach fizyki) poziomu bezpieczeństwa w komunikacji. W świetle znanych obecnie praw fizycznych (fundamentalnie kwantowych) jest to najdoskonalsza forma technologii kryptograficznej dla zastosowań obejmujących poufną komunikację, o istotnym znaczeniu ekonomicznym, ale również narodowym i strategicznym.

Koncepcyjna i technologiczna implementacja systemów kryptografii kwantowej, jedynego pewnego zabezpieczenia transmisji poufnych i integralnych danych w kanałach komunikacyjnych przed rozwijanymi komputerami kwantowymi, zagrażającymi klasycznym kryptograficznym systemom asymetrycznym (które stanowią niemal cały system nowoczesnych zabezpieczeń sieciowych dla zastosowań ekonomicznych, takich jak np. bankowość elektroniczna, transakcje sprzedaży i kupna, poufna komunikacja, uwierzytelnienie i autoryzacja), odbywa się w reżimie optyki kwantowej i wymaga bardzo precyzyjnych komponentów optyki kwantowej, obejmujących odp. tłumione lasery (źródła pojedynczych stanów kwantowych promieniowania elektromagnetycznego – możliwe również do implementacji przy wykorzystaniu splątania kwantowego), interferometry i polaryzatory, detektory pojedynczych fotonów (nośników informacji kwantowej) oraz światłowody i układy teleskopowe dla komunikacji w przestrzeni, jak również specjalne koncepcje architektury układów oraz implementacje sterujących systemów elektronicznych i ich oprogramowania interfejsowego. Nad tymi zagadnieniami w kontekście komercjalizacyjnym prowadzono w projekcie badania przemysłowe i prace rozwojowe, które zakończyły się sukcesem na poziomie prototypowych demonstratorów technologicznych, pilotażowych wdrożeń metropolitalnych w rzeczywistych środowiskach sieciowych oraz przygotowania do krajowej produkcji komercyjnych układów QKD.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

2. Geneza projektu

Rozwój społeczeństwa informacyjnego oraz gospodarki opartej na wiedzy stopniowo czyni z informacji podstawowy zasób ekonomiczny. Postępujące upowszechnienie w niemal każdej dziedzinie życia systemów informatycznych i telekomunikacyjnych skutkuje wirtualizacją wielu aspektów funkcjonowania społeczeństwa, gospodarki i państwa. Dotyczy to poza niezauważalnymi już procesami rozliczeń międzybankowych typu RTGS, gromadzących i przetwarzających całkowicie wirtualne środki finansowe na rachunkach osób fizycznych i prawnych, również w rosnącym stopniu komunikacji i koordynacji pracy najważniejszych jednostek organizacyjnych, w tak newralgicznych sektorach jak bezpieczeństwo prywatne i publiczne, obronność narodowa, ochrona zdrowia, reagowanie kryzysowe, zwalczanie przestępczości, etc. Rozwój i upowszechnianie technologii informatycznych z jednej strony znacząco zwiększa wydajność pracy i obniża jej koszty, podnosi dyfuzję innowacji w gospodarce i zwiększa jej konkurencyjność, niweluje bariery dostępu i upowszechnia edukację, przeciwdziałając także wykluczeniu społecznemu, z drugiej jednak strony zwiększa podatność funkcjonowania poszczególnych podmiotów, a także całego społeczeństwa, gospodarki i państwa na wpływ zewnętrznych czynników ingerujących w infrastrukturę informatyczną potencjalnie zakłócając ją w trzech podstawowych aspektach: poufności, wiarygodności i integralności komunikacji.

Kryptografia stosowana, mająca na celu zapewnianie poufności, wiarygodności i integralności przetwarzanych i komunikowanych danych, staje się w tym kontekście kluczowym elementem funkcjonowania nowego, informacyjnego modelu społeczno-gospodarczego, nabierając rosnącej wagi jako przedmiot szeroko prowadzonych na całym świecie prac badawczo-rozwojowych. Pomimo, że już w latach 20 XX wieku opatentowano teoretycznie bezwarunkowo bezpieczny system kryptografii symetrycznej (klucza prywatnego) one-time pad (będący rozwinięciem szyfru Vernama, stosującym jednorazowe, losowe klucze kryptograficzne o długości szyfrowanej wiadomości) – dowód podał w 1949r. Shannon, wkrótce po sformułowaniu podstaw teorii informacji – to jednak dotychczas nie udało się praktycznie rozwiązać towarzyszącego problemu dystrybucji klucza. Istotnie w trakcie prób jego rozwiązania w oparciu o uogólnienie podanej Diffiego i Hellmana w 1976r. metody, powstał całkowicie nowy model kryptografii asymetrycznej (klucza publicznego). Implementacje kryptograficzne w ramach tego modelu charakteryzują się własnością braku problemu dystrybucji klucza, który zastąpiony został parą kluczy: publicznym-jawnym (służącym do szyfrowania wiadomości przesyłanych do określonego odbiorcy) i prywatnym-poufnym (znanym tylko i wyłącznie odbiorcy i służącym do rozszyfrowywania otrzymywanych wiadomości). Para kluczy (publiczny i prywatny) jest ze sobą powiązana w sensie obliczeniowym problemem matematycznym o asymetrycznej złożoności (takim jak np. faktoryzacja liczby na czynniki pierwsze – operacja trudna w sensie teorii złożoności – względem której operacja odwrotna, tj. mnożenie liczb pierwszych – jest trywialna). Takie powiązanie umożliwia łatwe wygenerowanie klucza publicznego z klucza prywatnego, jednocześnie zapewniając wysoki poziom bezpieczeństwa tego drugiego (poprzez dużą złożoność obliczeniową procesu jego otrzymania na podstawie postaci jawnego klucza publicznego).

Matematyczne, obliczeniowe uwarunkowanie kryptografii asymetrycznej, która ze względu na swoją podstawową własność braku konieczności rozwiązania problemu dystrybucji klucza prywatnego pomiędzy wieloma stronami komunikacji, szybko rozpowszechniła się w powstających sieciach informatycznych, które ostatecznie wyewoluowały tworząc Internet, jest niekorzystne wobec ryzyka

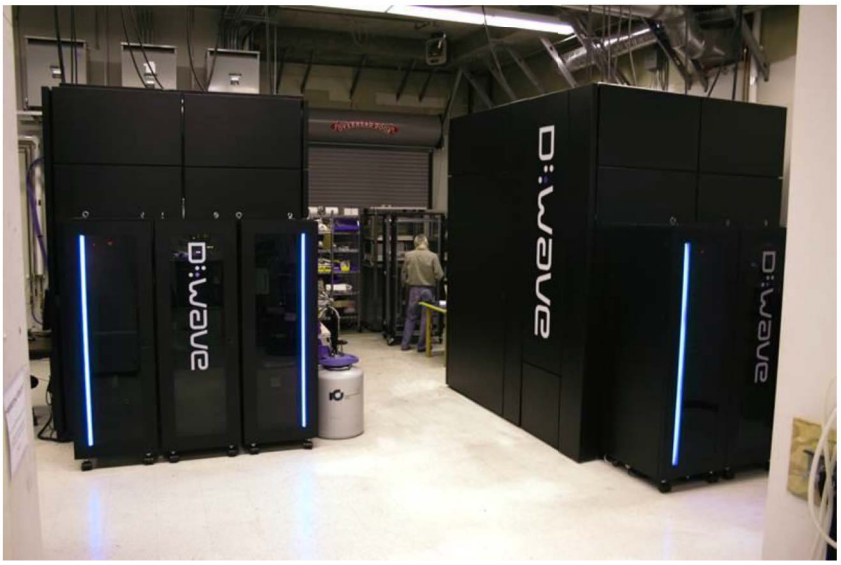
Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

wynalezienia algorytmów redukujących złożoność obliczeniową określonych problemów trudnych i natychmiast dezawuujących oferowane obecnie pozorne tylko bezpieczeństwo. Jakkolwiek w przypadku komercyjnego szyfru RSA, złamanie kluczy 1024-bitowych przy zastosowaniu znanych obecnie algorytmów klasycznych i zaawansowanych metod równoległego przetwarzania jest możliwe w racjonalnej skali 1 roku obliczeniowego, to już zastosowanie kluczy 2048-bitowych, czyni ten najpowszechniejszy kryptosystem praktycznie odpornym na konwencjonalny atak. Sytuacja zmieniła się po zaprezentowaniu przez Shora w 1994r. kwantowego algorytmu faktoryzacji o wykładniczym przyspieszeniu względem klasycznego odpowiednika (funkcjonującego w ramach informatyki kwantowej, tj. modelu obliczeniowego opartego na fundamentalnie odmiennych od klasycznych prawach mechaniki kwantowej i przetwarzającego qubity będące superpozycjami bitów). Poważne zagrożenie bezpieczeństwa kryptografii asymetrycznej zostało zauważone i jest obecnie nadal szeroko dostrzegalne (nawet pomimo tego, że eksperymentalny, uniwersalny komputer kwantowy, który udało się dotychczas zbudować funkcjonował w ograniczonym i nieskalowalnym modelu, daleko poza obszarem praktycznych zastosowań ze względu na dekoherencję). Z wyników badań teoretycznych w zakresie przyczyn dekoherencji (tj. wypływu informacji kwantowej poza układ) wynika, że budowa skalowalnego uniwersalnego komputera kwantowego będzie trudnym zadaniem, jednak ostatnie lata pokazały kilka przełomów w tym zakresie. W ostatniej dekadzie zademonstrowano tylko kilku-qubitowe komputery kwantowe w technologii NMR i spułapkowanych jonów – obydwie technologie nie pozwalają jednak na skalowanie do dużego komputera o praktycznym znaczeniu z uwagi na ograniczenia dekoherencyjne w drugim przypadku i ograniczenia przestrzenne spinowego układu jądrowego molekuł, w pierwszym. W marcu 2013 doniesiono o zbudowaniu w kanadyjskiej firmie D-Wave 512-qubitowego komputera kwantowego o skalowalnej architekturze w technologii nadprzewodnikowych złączy Josephsona: D-Wave Two (http://www.dwavesys.com/en/products-services.html). W przypadku tej konstrukcji nie jest jednak wykorzystywane splątanie kwantowe, a protokół kwantowego wyżarzania oparty na tunelowaniu elektronów w złączach Josephsona, pozwalający na szybkie (nieosiągalne klasycznie) rozwiązywanie zagadnień optymalizacyjnych – duże zainteresowanie wykazuje Google (inwestycja w kierunku kwantowego silnika wyszukiwarki obrazów, których rozpoznawanie wiąże się z podobnymi problemami jakie rozwiązywane są w algorytmach wyżarzania – dotyczy to wyszukiwania ekstremów w obrazach fourierowskich transformat) – w maju 2013 Google Inc. w konsorcjum z NASA zakupił większą ilość komputerów D-Wave Two w celu realizacji zaawansowanych badań nad sztuczną inteligencją (utworzenie przez Google i NASA kwantowego laboratorium sztucznej inteligencji) – wcześniej komputery D-Wace kupił m.in. główny koncern zbrojeniowy USA Lockheed-Martin (zakup pierwszej generacji D-Wave One do badań obliczeniowych za kwotę 10 mln USD). Ten gwałtowny skok technologiczny w dziedzinie komputerów kwantowych, bezpośrednio zagrażających klasycznym systemom kryptograficznym, stanowiącym podstawę wszelkich zabezpieczeń komunikacji elektronicznej, powoduje wzrost zainteresowania kryptografią kwantową - QKD, jako jedynym, zweryfikowanym zabezpieczeniem przed kwantowymi urządzeniami informatycznymi. Zagrożenie to jest tym bardziej poważne, że w przypadku skonstruowania pierwszego komputera kwantowego łamiącego uważane za bezpieczne algorytmy asymetrycznej kryptografii klasycznej, wszystkie informacje, których poufność została kiedykolwiek zabezpieczona przy użyciu takich lub podobnych metod (obecnie stanowiących podstawę niemal wszystkich praktycznie stosowanych zabezpieczeń w komunikacji elektronicznej) zostaną natychmiast ujawnione. Stanowi to główną przyczynę potrzeby jak najszybszej komercjalizacji kryptografii kwantowej, która dzięki prawom mechaniki kwantowej rozwiązuje w sposób teoretycznie bezwarunkowo bezpieczny, problem dystrybucji klucza w modelu

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

kryptografii symetrycznej, czyniąc z niej idealną technikę zabezpieczenia informacji, w sposób fundamentalny odporną na metody krypto-analityczne.

Wnętrze komputera D-Wave Two w kriogeniczej osłonie, widoczny nadprzewodzący procesor 512 qubitowy, wykorzystujący kwantowe tunelowanie elektronów w tzw. złączach Josephsona



Komputery D-Wave Two podczas pracy (takie same systemy zakupione zostały w maju b.r. przez firmę Google Inc. we współpracy z NASA oraz przez firmę Lockheed Martin)

Istotne przełomy w badaniach nad QIP wskazują, że postęp technologiczny w zakresie informatyki kwantowej oceniany przez bardziej optymistycznych ekspertów jest coraz bliżej skalowalnego komputera kwantowego i możliwe, że zostanie on zbudowany w skali umożliwiającej jego praktycznej zastosowanie w perspektywie krótko-terminowej (kilka lat) lub średnio-terminowej (kilkanaście lat). Nie brakuje jednak również sceptyków według których ewentualny przełom nastąpi w perspektywie długoterminowej (dziesięcioleci), a nawet, że być może z przyczyn fundamentalnych nie będzie w ogóle możliwy (ze względu na różnice pomiędzy światem klasycznym i kwantowym oraz ewentualną niedostępnością skalowalnych układów kwantowych dla świata, a więc również informacji klasycznych). Jednak bezsprzecznym pozostaje fakt, że ewentualny przełom w budowie komputera

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

kwantowego lub alternatywnie w algorytmice matematycznej (odkrycie nowych algorytmów lub innych modeli obliczeniowych, w których pewne asymetryczne problemy trudne zostaną zredukowane do łatwych, charakteryzujących się wielomianową złożonością), uczyni klasyczną kryptografię asymetryczną bezużyteczna w trybie natychmiastowym, a wszystkie informacje kiedykolwiek szyfrowane wg jej protokołów będą mogły zostać odczytane.

Stanowi to główną przyczynę rozważania możliwości komercjalizacji kryptografii kwantowej, która dzięki prawom mechaniki kwantowej rozwiązuje w sposób teoretycznie bezwarunkowo bezpieczny, problem dystrybucji klucza prywatnego w modelu kryptografii symetrycznej. Zaproponowany przez Bennetta i Brassarda w 1984r. (na podstawie *postulowanego* w latach 60 pomysłu odpornych na podrabianie kwantowych pieniędzy Wiesnera) protokół QKD (Quantum Key Distribution) jest jedną z najbardziej perspektywicznych koncepcji kryptograficznych. Pomimo długiego okresu jaki upłynął od podania protokołu BB84 (i jego rozwinięcia podanego przez Bennetta w 1992r., tj. protokołu B92), a także bardziej zaawansowanej koncepcji kryptografii kwantowej opartej o splątanie (przedstawionej przez Ekerta w 1991r. i znanej obecnie jako protokół E91), wysoki poziom wymaganej precyzji realizacji eksperymentu kwantowego oraz związane z tym koszty i ograniczenia technologiczne w zakresie optyki kwantowej stanowiły skuteczną barierę dla szerokiej komercjalizacji kryptografii kwantowej. Istotny postęp technologiczny w optyce kwantowej urealnił komercjalizację kryptografii kwantowej dopiero kilka lat temu, a zrealizowany projekt przyczynia się do postępu w tej dziedzinie.

W kontekście metodologicznym kryptografia kwantowa, a ściślej kwantowa dystrybucja klucza QKD jest technologią z zakresu przetwarzania informacji kwantowej (QIP, Quantum Information Processing) – jak już wspomniano dziedziny leżącej na przekryciu fizyki kwantowej i informatyki. Wykorzystanie kwantowego nośnika informacji prowadzi do licznych przewag nad jej klasycznym odpowiednikiem obecnie używanym w informatyce. Pośród spektakularnych realizacji QIP wymienić można komputer kwantowy, kwantową teleportację i właśnie QKD. Idea QKD jest klasyfikowana w obszarze kryptografii symetrycznej (lub kryptografii klucza prywatnego), w której pomiędzy zmiennymi parametrami algorytmu szyfrującego oraz algorytmu deszyfrującego (tzw. kluczami) istnieje pewna symetria, w szczególności symetria identycznościowa. Już w latach 20 ubiegłego wieku opatentowano w USA teoretycznie bezwarunkowo bezpieczny system kryptografii symetrycznej nazwany one-time pad (OTP), stanowiący rozwinięcie szyfru Vernama poprzez zastosowanie jednorazowych, losowych kluczy kryptograficznych o długości szyfrowanej wiadomości – dowód podał w 1949r. Shannon, twórca teorii komunikacji. Algorytm ten (o prostej implementacji operacji logicznej XOR, tj. sumy bitowej modulo 2 lub tzw. wykluczającej alternatywy na poszczególnych pozycjach bitowych wiadomości i klucza) oferuje niezawodny (oraz całkowicie odporny na wszelkie możliwe do zastosowania techniki krypto-analityczne) poziom bezpieczeństwa poufności komunikacji przy założeniu stosowania klucza o długości równej długości wiadomości oraz o całkowitej losowości. Klucz ten musi być jednak współdzielony przez obie strony komunikacji, co oznacza, że w jakiś sposób musi zostać pomiędzy te strony rozdystrybuowany – jak dotychczas nie udało się praktycznie rozwiązać tego problemu w sposób bezwarunkowo bezpieczny w oparciu o prawa fizyki klasycznej, a ponadto udowodniono, że jest to niemożliwe – jedynie prawa mechaniki kwantowej pozwalają znaleźć rozwiązanie tego problemu (co zostało zweryfikowane empirycznie już niemal 30 lat temu w 1984 roku). W trakcie prób rozwiązania kwestii bezpiecznej dystrybucji klucza prywatnego w oparciu o uogólnienie podanej w 1976r. przez Diffiego i Hellmana klasycznej metody kryptograficznej (jednak o warunkowym bezpieczeństwie), wyodrębniła się nowa gałąź kryptografii nazwana asymetryczną (lub też kryptografią klucza publicznego). Model asymetrycznych krypto-systemów charakteryzuje się

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

brakiem konieczności realizacji procedur dystrybucji klucza, który został zastąpiony parą kluczy: tzw. publicznym – jawnym (przypisany do określonego odbiorcy i służący do szyfrowania wiadomości przesyłanych do niego) i prywatnym – poufnym (znanym wyłącznie odbiorcy i służącym do rozszyfrowywania otrzymywanych wiadomości). Oba klucze w parze są ze sobą powiązane w sensie obliczeniowym problemem matematycznym o asymetrycznym charakterze złożoności (takim jak np. rozkład, tj. faktoryzacja liczby na czynniki pierwsze – operacja trudna w sensie teorii złożoności obliczeniowej – względem której operacja odwrotna, tj. mnożenie liczb pierwszych, jest obliczeniowo trywialna). Tego typu asymetryczna zależność matematyczna obu kluczy zapewnia wysoki poziom bezpieczeństwa szyfrowanych danych dzięki dużej złożoności obliczeniowej procesu otrzymywania deszyfrującego klucza prywatnego na podstawie postaci jawnego, szyfrującego klucza publicznego (należy podkreślić, że powyższy jedynie warunkowo bezpieczny schemat został z powodzeniem wykorzystany przy niewielkich uzupełnieniach o stosowanie tzw. funkcji mieszających w sposób odwracający role kluczy dla zastosowań uwierzytelniających – tj. tzw. podpisu cyfrowego – w miejsce obecnie również bardzo upowszechnionych zastosowań zapewniających poufność komunikacji).

Pomimo, że pierwszy protokół kryptografii kwantowej (kwantowej dystrybucji klucza, QKD) został zaproponowany przez Bennetta i Brassarda już w 1984r. (idea kryptografii kwantowej opierała się na postulowanym w latach 60 przez Wiesnera pomyśle kwantowego znakowania banknotów), to dopiero obecny poziom rozwoju technologii umożliwia badania przemysłowe i komercjalizację tych koncepcji (szeroko rozwijanych także w wymiarze protokołów i zastosowań). Teoretycznie absolutne bezpieczeństwo kwantowego przekazu klucza opiera się na podstawowych zasadach mechaniki kwantowej – jest to niezwykła i nieosiągalna nigdy wcześniej własność kryptograficzna, rewolucyjna dla teorii komunikacji (podobnie rewolucyjna jest nielokalna własność korelacyjna splątania kwantowego, które umożliwia teleportację kwantową stanów kwantowych materii na odległość, a także nielokalną komunikację informacji klasycznej za pośrednictwem kanałów kwantowych, w których komunikowana informacja nie może być przechwycona co zapewniają fundamentalne własności mechaniki kwantowej – jest to niezrozumiały klasycznie fenomen komunikacji nielokalnej).

Własności te opierają się strukturze algebraicznej mechaniki kwantowej oraz na własnościach pomiaru kwantowego, tj. rzutowania von Neumanna – schematu eksperymentu w kwantowej mechanice polegającego na kolapsie stanu kwantowego w trakcie mierzenia, czego konsekwencją jest niemożliwość skopiowania nieortogonalnych stanów kwantowych i tzw. zakaz klonowania będący podstawą protokołów QKD. Wynik rzutowania von Neumanna jest absolutnie przypadkowy (losowość kwantowa) i dlatego niemożliwy do przewidzenia w przeciwieństwie do pseudolosowych rozkładów używanych w klasycznej informatyce (odzwierciedlających specyfikę chaotycznych procesów klasycznych, podlegających jednak deterministycznemu opisowi równań ewolucji układu). Te ostatnie mogą być teoretycznie przewidziane przy wystarczających zasobach informatycznych, to jednak kwantowe – nie. Rzutowanie von Neumanna nie jest w pełni zrozumiane do tej pory (co wiąże się z niezrozumieniem granicy pomiędzy tak odmiennymi światami kwantowym i klasycznym), pomimo, że nad jego zrozumieniem od niemal 100 lat pracowali najwybitniejsi naukowcy na świecie. Jest ono traktowane jest jako podstawowe założenie kwantowego obrazu świata, i mimo, że nie w pełni zrozumiane (jednak z następującym postępem np. w zakresie teorii superwyboru Wojciecha Żurka) – to jednak ponad wszelką wątpliwość potwierdzone doświadczalnie wraz z pewnością co do złamania założeń lokalnego-realizmu przez mechanikę kwantową.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

3. Cel główny projektu

Celem głównym projektu w ramach I etapu działanie 1.4. PO IG było rozpoznanie możliwości i uwarunkowań technicznych oraz przygotowanie do wdrożenia i komercjalizacji układów kryptografii kwantowej splątaniowej i bezsplątaniowej, tj. wykorzystującej protokoły zarówno nieoparte jak i oparte na splątaniu kwantowym. Uwarunkowania techniczne obecnego stanu rozwoju optyki kwantowej dla celów zastosowań w rzeczywistych sieciowych środowiskach komercyjnych były rozpoznawane poprzez przeprowadzenie badań przemysłowych i prac rozwojowych w warunkach laboratoryjnych. Celem ogólnym projektu był długofalowy wzrost konkurencyjności oferty realizatora projektu na rynku komercyjnym poprzez przygotowanie technologiczne realizatora projektu do wprowadzenia innowacyjnych, strategicznych i perspektywicznych produktów oraz usług do swojej oferty komercyjnej, a także w dłuższej perspektywie wzrost przychodów i rentowności firmy po wdrożeniach komercyjnych planowanych po zakończeniu realizacji projektu w okresie jego trwałości. Istotnym celem projektu był również sam rozwój i ogólne przemysłowe wdrożenie innowacyjnej technologii kryptografii kwantowej, która ma duży potencjał dla unowocześnienia i zwiększenia konkurencji gospodarki krajowej względem gos podarek państw wysoko rozwiniętych.

Zgodnie z założeniami projektu po realizacji fazy badawczo-rozwojowej, w oparciu o uzyskane wyniki badań i prototypową technologię planowano produkcyjne wdrożenie do sprzedaży polskich układów kryptografii kwantowej na międzynarodowym rynku komercyjnym i przygotowanie na tej podstawie produktowej oferty rynkowej układów kryptografii kwantowej (bezsplątanowej i splątaniowej), przy dodatkowym wsparciu finansowym (pierwotnie zgodnie ze specyfiką działania 1.4/4.1 PO IG, planowanym w ramach odrębnego projektu w działaniu 4.1 PO IG stanowiącego formalnie II etap projektu, jednak ze względu na zakończenie perspektywy finansowej i brak możliwości uzyskania wsparcia w zamkniętym działaniu 4.1 PO IG, w oczekiwaniu adekwatnych możliwości programowego wsparcia działań wdrożeniowo-inwestycyjnych – obejmującego głównie przygotowanie do produkcji zintegrowanych układów opartych na zminiaturyzowanych rozwiązaniach prototypowych – w ramach PO IR oraz programów celowych NCBiR – m.in. programu inwestycyjnego Brigde Venture Capital).

4. Opis przeprowadzonych badań przemysłowych

Koncepcja kryptografii kwantowej jest wynikiem jednych z najbardziej obiecujących pod względem potencjału aplikacyjnego, naukowych badań podstawowych, prowadzonych w dziedzinach fizyki i informatyki w przeciągu trzech ostatnich dekad. Oferując teoretycznie bezwarunkową ochronę (w przeciwieństwie do ochrony warunkowej ze strony kryptografii klasycznej, opartej na problemach matematycznie trudnych) niejawnej komunikacji prowadzonej w ramach modelu P2P (peer-to-peer lub punkt-do-punktu), ma istotne znaczenie dla strategicznego bezpieczeństwa kraju oraz duży potencjał komercjalizacyjny (także w skali międzynarodowej). Nawet przy uwzględnieniu fizycznych niedoskonałości implementacyjnych kryptografia kwantowa stanowi jakościowo nową klasę bezpieczeństwa w ramach procedury kwantowej dystrybucji klucza, która w połączeniu z podstawowym modelem kryptografii symetrycznej one-time pad (OTP), lub zoptymalizowanymi kryptosystemami podstawieniowo-permutacyjnymi nowej generacji typu AES czy 3DES, zapewnia najwyższy dostępny obecnie poziom skuteczności ochrony przesyłania informacji niejawnych pomiędzy dwiema stronami komunikacji. Pomimo dużego postępu prac badawczo-rozwojowych nad

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

kryptografią kwantową na świecie, w kraju brak jest znaczących przedsięwzięć na poziomie badań przemysłowych i postępu technicznego w tym obszarze. Zaawansowane prace wdrożeniowe prowadzone są m.in. w Europie w dwóch wiodących ośrodkach naukowo-przemysłowych w tej dziedzinie tj. w Genewie (Uniwersytet Genewski i firma idQuantique SA pod kierunkiem prof. Gisina) oraz w Wiedniu (Uniwersytet Wiedeński i Centrum Kwantowej Optyki, Nanotechnologii i Informacji oraz Austrian Institute of Technology, pod kierunkiem prof. Zeilingera). Poza Europą prace rozwojowe i badania przemysłowe prowadzone są także w Stanach Zjednoczonych (BBN Technologies, MagiQ) i w Japonii (NEC, Toshiba, która ma także centrum w Cambridge w Anglii), a prace eksperymentalne i badawcze o charakterze podstawowym realizowane są na wielu tamtejszych uczelniach wyższych.

Prace badawcze w projekcie objęły 4 prototypowe układy kryptografii kwantowej (kwantowej dystrybucji klucza QKD). Dwa pierwsze prototypy to splątaniowe układy QKD niskiego poziomu integracji opto-elektronicznej, które umożliwiają także bezsplątaniowy tryb działania. Pierwszy prototyp w tej grupie to splątaniowy układ QKD stacji nadawczo-odbiorczej (w konwencji teorii komunikacji - Alice), a drugi prototyp to splątaniowy układ QKD stacji odbiorczej (w konwencji teorii komunikacji - Bob). Prototypy te zaimplementowane zostały w technologii makroskopowych, otwartych układów optyki kwantowej powstałych w toku realizacji badań na bazie szkieletowych platform badawczo-rozwojowych QKD AIT zakupionych jako zintegrowane komponenty opto-elektroniczne konieczne do realizacji protokołu QKD w projekcie. Wszystkie elementy składowe (tj. komponenty optyczne i elektroniczne) prototypowych układów splątaniowych QKD, które mogą także realizować tryb bezsplątaniowy) są komercyjnie dostępne i stanowią podstawę materiałową (półprodukty) dla planowanej linii produkcyjnej komercjalizowanych układów splątaniowych QKD opartych na prototypach optymalizujących działanie procedur QKD wypracowanych w toku realizacji zadań projektowych (architektury protokołowe podlegające procedurom ochrony patentowej). Prototypowe układy splątaniowe QKD realizują kodowanie informacji kwantowej na splątaniach polaryzacyjnych stopni swobody fotonów przy wykorzystaniu procesu spontanicznej parametrycznej konwersji w dół (SPDC) w oparciu o nieliniowe efekty w kryształach BBO (beta boranu baru). Szczegółowy opis prototypów splątaniowych układów QKD znajduje się w ich dokumentacji technicznej.

Dwa kolejne prototypy to bezsplątaniowe układy QKD wyższego poziomu integracji opto-elektronicznej. Pomimo, że nie jest to jeszcze poziom integracji chipowej w układach scalonych, to jednak drogi optyczne (w reżimie optyki kwantowej) są w tych protypach w pełni zamknięte w układach światłowodowych i komponentach opto-elektronicznych (w tym w źródłach laserowych i detektorach pojedynczych fotonów). Wynika to z braku konieczności stosowania procedury SPDC, która na obecnym poziomie rozwoju technologii optyki kwantowej została zrealizowana eksperymentalnie tylko w reżimie otwartej drogi optycznej - tj. koherentnej wiązki laserowej padającej na makroskopowy kryształ BBO, z którego wychodzą dwa stożki świetlne o przeciwnych polaryzacjach, generując pary splątane na przecięciu ich krawędzi. Brak konieczności stosowania makroskopowych procesów nieliniowych w krysztale BBO w otwartej drodze optycznej powoduje możliwość integracji układów opto-elektronicznych. Oba prototypy bezsplątaniowe implementują kodowanie informacji kwantowej na przesunięciach fazy fotonów w losowo zestawianych krótkich i długich drogach optycznych (będących ramionami interferometru Macha-Zehndera). Taka też realizacja kodowania kwantowego jest znacznie odporniejsza na procesy dekoherencyjne związane z depolaryzacją silnie obecną w światłowodzie. Prototypy układów bezsplątaniowych QKD kodujące

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

informacje na fazie, zaimplementowane zostały w oparciu o platformy B+R zintegrowanych układów opto-elektronicznych IDQuantique umożliwiających sterowanie elektroniczne komponentami optyki kwantowej. Wszystkie komponenty składowe prototypów, na których prowadzono modyfikacje i optymalizacje protokołowe oraz architekturowe – są w pełni dostępne komercyjnie ale ich integracja seryjna jest procesowo znacznie bardziej złożona niż integracja seryjna układów splątaniowych QKD. Planowana linia produkcyjna układów bezsplątaniowych kodowania fazowego przy uwzględnieniu wypracowanych w projekcie koncepcji architektoniczno-protokołowych jest też z tego powodu bardziej kosztowna i pracochłonna niż w przypadku splątaniowych układów QKD. Z kolei jednak półprodukty materiałowe są tańsze ze względu na wykorzystanie znacznie mniejszej liczby dedektorów pojedynczych fotonów (są to najdroższe komponenty układów) oraz brak układu SPDC generowania splątania kwantowego; jest to również jednostkowo kosztowny i wrażliwy komponent optyki kwantowej. Pierwszy prototyp bezsplątaniowy QKD zawiera źródło oraz detektor, stanowiąc stację nadawczo-odbiorczą (Bob). Drugi z kolei zwierciadło Faradaya i detektor, stanowiąc stację odbiorczą (Alice). Szczegółowy opis prototypów bezsplątaniowych układów QKD znajduje się w ich dokumentacji technicznej.

Badania przemysłowe i prace rozwojowe przeprowadzone w ramach projektu stanowiły ważne i międzynarodowo dostrzeżone uzupełnienie prac badawczo-rozwojowych i badań podstawowych prowadzonych na świecie. Ich istotną cechą było skupienie interdyscyplinarnego zespołu badawczego (fizyków i informatyków) w zakresie prac eksperymentalnych nad układami QKD zarówno splątaniowymi jak i bezsplątaniowymi – badania takie, obejmujące prace interdyscyplinarnego zespołu badawczego zarówno nad splątaniowymi i bezsplątaniowymi układymi kryptografii kwantowej nie były dotychczas prowadzone. Ich rezultaty (podlegające obecnie procedurom zapewnienia ochrony patentowej przy wsparciu programu PatentPlus NCBiR) pozwoliły na skuteczną identyfikację perspektywicznych technologicznych kierunków komercjalizacji kryptografii kwantowej w kraju i na rynku międzynarodowym.

Realizowane badania przemysłowe były ulokowane w zakresie następującej problematyki technologicznej kryptografii kwantowej, stanowiącej najważniejsze bariery w jej komercjalizacji:

1. Niedoskonałości źródeł niesplątanych fotonów jako kwantowych nośników informacji (wysoce tłumione lasery, które efektywnie nie są w stanie emitować jednofotonowych impulsów przy zapewnieniu wysokiej częstości operacji determinującej efektywność transmisji i przez to są podatne na ataki klasy PNS photon number splitting, wykorzystujące większą niż 1 liczbę fotonów w tłumionym impulsie elektromagnetycznym; w tym kontekście istotne są prace zespołów, które doniosły w ostatnim czasie o znalezieniu i wykorzystaniu luk bezpieczeństwa obecnych w komponentach optycznych bezsplątaniowej QKD).
2. Niedoskonałości źródeł splątanych par fotonów jako kwantowych nośników informacji ujawniające się w postaci obniżonych statystycznych wartości oczekiwanych korelacji wyników pomiarów (zbliżających się do granicy nierówności Bella lub nierówności CHSH na nieklasyczne korelacje w zakresie wyników pomiaru) w obliczu uwarunkowań i ograniczeń technologicznych procedur puryfikacji i destylacji splątania kwantowego.
3. Niedoskonałości kanałów kwantowych i dekoherencja kwantowych nośników informacji kodowanych na polaryzacjach fotonów, ograniczające zasięg i podnoszące poziom błędów w transmisji, tzw. QBER, quantum bit error rate (problemy z kolimacją wiązki w przypadku kanałów w powietrzu lub w próżni, czy też rozproszeniami w ośrodkach i dwójłomnością

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

światłowodów w przypadku światłowodowych linii transmisyjnych, fundamentalny charakter dekoherencji i jej własności wykładniczego wzrostu w powiązaniu z naturą oddziaływań kwantowych; także w aspekcie technologicznym dotyczącym uwarunkowań sieci miejskich).

4. Niedoskonałości detektorów kwantowych pojedynczych fotonów (tj. nośników informacji w kanale kwantowym) działających w oparciu o diody lawinowe (problem tzw. ciemnych zliczeń); podatność na specjalne klasy ataków (doniesienia zespołów badawczych z Norwegii i Kanady o skuteczności klasy ataków wykorzystujących niedoskonałości techniczne detektorów z diodami lawinowymi poprzez ich intensywną iluminację i oślepienie).
5. Ograniczenia natury topologicznej względem układów połączeń sieciowych dystrybucji klucza kwantowego (topologia P2P, tj. punkt-do-punktu) w powiązaniu z barierami fundamentalnymi (twierdzenie no-cloning Żurka o zakazie kopiowania informacji kwantowej) oraz zagadnieniami praktycznymi w zakresie standaryzacji i integracji interfejsowej (na poziomie warstwy łącza fizycznego modelu ISO/OSI oraz wyższych warstw w zakresie problematyki integracji z protokołami sieci internetowych w tym w szczególności warstwy sieciowej i stosu protokołowego IP/IPSec, służącego zabezpieczeniu protokołów transportowych w Internecie: protokołu TCP lub UDP oraz protokołów warstwy aplikacyjnej).
6. Ograniczenia związane z problemem uwierzytelnienia w ramach sesji kryptografii kwantowej i podatność na ataki klasy *man-in-the-middle* polegające na przechwyceniu kanałów kwantowego i klasycznego oraz impersonifikacji jednej ze stron komunikacji (problem redukcji protokołów QKD quantum key distribution do QKE quantum key expansion).

W projekcie zrealizowano następujące zadania w zakresie zaplanowanych badań przemysłowych:

Zadanie 1. Zbadanie technicznych uwarunkowań źródeł niesplątanych nośników kwantowych i możliwości kodowania na nich informacji w układach QKD bezsplątaniowych (typu BB84 lub B92).

W toku zadania realizowane były badania w obszarze optymalnych konfiguracji komponentów zintegrowanych układów optyki kwantowej generujących pojedyncze fotony oraz umożliwiających zadanie stanów superpozycji kwantowych. Kodowanie informacji kwantowej koniecznej w protokołach BB84 i B92 odbywało się w układach interferometrycznych na przesunięciach fazowych fotonów propagujących się drogami optycznymi o różnych długościach w zestawianych losowo (w reżimie mechaniki kwantowej) ramionach interferometrów Macha-Zehndera. W toku zadania prowadzono analizy parametrów źródeł pojedynczych fotonów w postaci silnie tłumionych diód laserowych. Przeprowadzono badania w zakresie rozkładów statystycznych prawdopodobieństw dystrybucji fotonów (preferencyjnie znalezienia się co najwyżej 1 fotonu) w tłumionym impulsie laserowym dla zapewnienia podstawowego paradygmatu kryptografii kwantowej opartego na zaburzeniu stanu układu kwantowego wprowadzanego przez pomiar. Stan kwantowy pojedynczego fotonu (np. jego polaryzacji lub przesunięcia fazowego) nie może być zmierzony bez wprowadzenia statystycznie wykrywalnego zaburzenia (ze względu na brak znajomości bazy pomiaru, związanej np. w układzie polaryzacyjnym z osią polaryzacji, lub w układzie interferometrycznym z całkowicie losowym, w reżimie niedeterministycznej losowości kwantowej /przy wykluczeniu luki deterministycznej pseudolosowości klasycznej/, wyborze drogi optycznej poprzez rozdzielacze wiązek). Dlatego tak istotnym elementem praktycznej kryptografii kwantowej jest zapewnienie rzeczywiście pojedynczych stanów kwantowych (fotonów) w laserowych impulsach komunikacyjnych, co osiąga się przez wysoki poziom tłumienia intensywności światła (ze statystyczną dystrybucją co najwyżej 1 fotonu na impuls). Przeprowadzono testy tłumionych źródeł pojedynczych stanów

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

kwantowych względem możliwości zastosowania ataków typu PNS (Photon Number Splitting). Ponadto w zadaniu prowadzono powiązane testy parametrów technicznych prototypowych układów źródeł stanów splątanych dla kryptografii kwantowej bezsplątaniowej (w tym eksperymentalne realizacje protokołów QKD nieopartych na splątaniu kwantowym w środowisku laboratoryjnym). Badania prowadzono w oparciu o eksperymentalnie uruchomiony prototypowy bezsplątaniowy układ QKD w postaci platformy B+R komponentów interferometrycznych układów optyki kwantowej. Komponenty te obejmują źródło laserowe, cyrkulator, detektor kwantowy i klasyczny konieczny do zapobiegania tzw. atakom oślepiającym, modulatory fazy, układy tłumienia optycznego, światłowody opóźniające, lustro Faradaya oraz komponenty elektroniczne sterowania zintegrowanymi układami optyki kwantowej. Architektura układu prototypowego rozdziela komponenty optyki kwantowej na 2 stacje: nadawczą (Bob) i odbiorczą (Alice) dystrybucji klucza QKD (stacja nadawcza, choć na poziomie technicznym pełni również funkcje odbiorcze, tj. detekcji kwantowej, jest wyposażona w większość komponentów optyki kwantowej w tym źródła i detektory, podczas gdy stacja odbiorcza wyposażona jest przede wszystkim w lustro Faradaya oraz dodatkowo w układy tłumienia, środkowoprzepustowy filtr, rozdzielacz wiązki, modulator fazy i światłowód opóźniający dla układu interferometrycznego). W ramach problematyki pojedynczych stanów kwantowych w impulsie (pojedynczych fotonów w impulsie laserowym), która bezpośrednio odnosi się do podatności na najważniejszą klasę ataków na implementacje QKD (ataki PNS), prowadzono także badania w obszarze zastosowania splątania kwantowego do zagwarantowania propagacji pojedynczego stanu kwantowego (podejście to zostało szczegółowo zweryfikowane w ramach zadania 2, jako że przekrywa się z badaniem uwarunkowań technologicznych dla źródeł splątanych fotonów w procesie parametrycznej konwersji w dół wiązki w kryształach nieliniowych. Należy podkreślić, że badania w zakresie zadania 1. zostały przeprowadzone także w reżimie kodowania informacji kwantowej na stanach polaryzacyjnych w ramach 2 innych prototypowych układów optyki kwantowej rozwijanych głównie w celu realizacji badań w ramach zadania 2. Szczegółowe rezultaty badań w zakresie zad. 1. zebrano w prezentacjach konferencyjnych i w publikacjach na temat uwarunkowań technicznych bezsplątaniowych układów QKD (w częściach dotyczących charakterystyk źródeł qubitów w kanałach kwantowych oraz pośrednio w zakresie ogólnych parametrów transmisyjnych).

Zadanie 2. Zbadanie technicznych uwarunkowań źródeł splątanych nośników kwantowych i możliwości kodowania na nich informacji w układach QKD splątaniowych (typu E91).

W zadaniu realizowane były badania w zakresie optymalnych konfiguracji wiązek optycznych w układach optyki kwantowej generujących splątanie stanów polaryzacyjnych fotonów w procesie SPDC, spontanicznej parametrycznej konwersji w dół w nieliniowych kryształach beta boranu baru o wysokich parametrach dwójłomności optycznej. Przedmiotem badań nie były badania własności i zastosowań samego splątania kwantowego (w tym innowacyjnych zastosowań kryptograficzno-komunikacyjnych), ale przede wszystkim optymalizacja wydajnościowa i parametryzacyjna procesu produkcji splątania. Przemysłowe badania laboratoryjne polegały głównie na testowaniu konfiguracji układu komponentów optycznych wymaganych dla procesu SPDC w eksperymentalnym zestawieniu układów optyki kwantowej sterowanych elektronicznie dla implementacji procedury kwantowej dystrybucji klucza w oparciu o efekt splątania kwantowego. Prototypowe układy splątaniowej QKD są w znacznie mniejszym stopniu zintegrowane niż prototypowe układy bezsplątaniowe ze względu na brak dostępności integrowalnych i zminiaturyzowanych komponentów generujących splątanie kwantowe i w związku z tym konieczność implementacji tego procesu na wolnej drodze optycznej w makroskopowych układach optyki kwantowej przy jej obecnym stanie rozwoju technologicznego – z

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

wykorzystaniem makroskopowego nieliniowego kryształu beta boranu baru w układzie mechanicznym z kompensacją dryfu wiązki laserowej). Niższy poziom integracji optyki kwantowej powoduje niższą stabilność układu (ze względu na zewnętrzne czynniki, przede wszystkim mikro-wibracje mechaniczne oraz fluktuacje termiczne) w toku rozkalibrowywania się precyzyjnie zadanej wiązki fotonów poprzez mechaniczne zestrojenie geometryczne drogi optycznej. Powoduje to ogólnie niższe parametry transmisyjne dla procedur kwantowej dystrybucji klucza QKD i gorszą stabilność niż w przypadku silniej zintegrowanych optycznie (ze względu na możliwości technologiczne i dostępność zintegrowanych potrzebnych elementów optyki kwantowej) układów bezsplątaniowych. W toku zadania badania przemysłowe obejmowały pośrednio charakterystyki samego splątania fotonów, jednak w zakresie analiz korelacji kwantowych (o nielokalnym charakterze) i weryfikacji ilościowej złamania nierówności Bella (w tym nierówności CHSH) na limit klasycznych korelacji statystycznych dla wartości oczekiwanej nieliniowej zmiennej losowej utworzonej z par obserwabli (polaryzacji fotonów) prowadzone były poza projektem odrębne, szczegółowe badania w kierunku zastosowań i rozwoju splątania kwantowego dla celów komunikacji (w tym także supergęstego kodowania kwantowego dla bezpośredniej nielokalnej i przez to bezpiecznej – bo nieniosącej w kanale komunikacyjnym w sposób lokalny informacji – komunikacji kwantowej). Badania przemysłowe uwarunkowań źródeł splątanych nośników kwantowych (w tym z podstawową analizą poziomu splątania kwantowego) obejmowały metody przeciwdziałania dekalibracji, przede wszystkim poprzez kompensację dryfu wiązki dla uzyskania możliwie najwyższych parametrów transmisyjnych i stabilnościowych w zastosowaniu procedur kwantowej dystrybucji klucza QKD przy wykorzystaniu splątania w polaryzacji fotonów. Prototypowy układ splątaniowy rozdzielony został na 2 stacje: nadawczą i odbiorczą. W stacji nadawczej umieszczono standardowe komponenty układu generującego splątanie w procesie SPDC (silnie pompowaną wiązkę laserową padającą w konfiguracji soczewek i filtrów w wolnej drodze optycznej na kryształ BBO beta boranu baru rozdzielający następnie wiązkę na dwie osobne odpowiednio polaryzowane drogi optyczne przy właściwej geometrycznej kalibracji punktów przecięcia stożków świetlnych z kryształu, w których to punktach nie istnieje możliwość rozróżnienia polaryzacji – fotony z tych dwóch punktów przecięć krawędzi stożków świetlnych są parami splątane w swoich stanach polaryzacji i są kierowane w drodze optycznej do osobnych światłowodów – jeden do układu detekcyjnego w stacji nadawczej, a drugi do światłowodu transmisyjnego lub do soczewek układu teleskopowego, który ma zadanie umożliwiać komunikację w przestrzeni), jak również komponenty detekcyjne (dla ominięcia istotnej problematyki negatywnego wpływu na układ mechanicznych lub piezolektycznych wariatorów baz pomiaru kwantowego w detekcji wykorzystano czysto optyczny układ statyczny oparty na kostkach światłodzielących – rozdzielaczach wiązki – oraz 4 detektorów pojedynczych fotonów na każdą stację, po 2 na każdą dwuwymiarową bazę pomiaru kwantowego polaryzacji fotonu; detektory pojedynczych fotonów oparte na technologii diod lawinowych stanowią najbardziej zaawansowane technicznie komponenty optyki kwantowej – ich uwarunkowania technologiczne były szczegółowo badane w kolejnych zadaniach, jednak ze względu na reżim optyki kwantowe służyły one także pośrednio do badań charakterystyk źródeł). Badania technicznych uwarunkowań źródeł splątanych fotonów były prowadzone w podstawowym zakresie analiz statystycznych nielokalnych korelacji wyników pomiarów własności rozseparowanych kauzalnie układów fizycznych (niezależnych w sensie przyczynowo-skutkowym, tj. w odpowiedniej odległości względem separacji czasowej aktu pomiaru, tak aby niemożliwe było wpłynięcie wyników pomiaru jednego układu na wyniki pomiaru drugiego przy uwzględnieniu maksymalnej prędkości światła dla rozchodzenia się oddziaływań w przestrzeni). W badaniach, w toku optymalnych konfiguracji układu optyki kwantowej oraz kluczowych systemów

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

sterowania udało się uzyskać wysokie wartości nielokalnych korelacji statystycznych co pośrednio świadczy o wysokim poziomie wierności eksperymentalnie generowanych par splątania kwantowego. Główny problem badawczy koncentrował się na stabilności produkcji splątania kwantowego dla celów zastosowań splątaniowych układów QKD w komercyjnych środowiskach sieciowych w kierunku ich komercjalizacji (badania prowadzone w tym obszarze miały swoją kontynuację w kolejnych zadaniach, jako że dla ostatecznych parametrów zastosowań stanów kwantowych w protokołach QKD liczą się nie tylko charakterystyki źródeł, ale również charakterystyki kanałów kwantowych i detektorów pojedynczych stanów kwantowych – oszacowano ograniczenia infrastrukturalne dla akceptowalnych poziomów parametrów transmisyjnych w toku testów prototypowego układu w telekomunikacyjnej sieci metropolitalnej). Ważny techniczny problem badawczy stanowiła kwestia synchronizacji okien czasowych detekcji dla identyfikacji par fotonów znajdujących się w kwantowym stania splątania. Badania w tym zakresie (realizowane przy współpracy z AIT Wiedeń, dostawcą komponentów układów optyki kwantowej dla realizacji procesu SPDC) pozwoliły na uzyskanie wysokich (na poziomie najbardziej zaawansowanych eksperymentalnych badań światowych) wartości statystycznych rozdzielczości czasowej splątanych par polaryzacyjnych, dzięki wydajnej (o wysokiej rozdzielczości) synchronizacji na drodze znakowania czasowego. Kodowanie informacji kwantowej w ramach kanału kwantowego eksperymentalnego stanowiska badawczego było realizowane na stanach polaryzacyjnych, które charakteryzują się względnie wyższą wartością dekoherencji niż stany modulacji fazowej (depolaryzacja wiąże się z nieuniknioną optyczną dwójłomnością ośrodków propagacji fotonów w formie światłowodów, ale jest też intensywna w innych ośrodkach, takich jak np. powietrze dla wolnej wiązki w atmosferze). Problematyka badania dekoherencji polaryzacyjnej była szczegółowo podjęta w kolejnych zadaniach badawczych (choć już w zadaniu 1. była przedmiotem wstępnych badań dla zapewnienia optymalnych charakterystyk jakości produkcji splątania kwantowego w źródłach wysyłających qubity splątaniowe w układach QKD). Szczegółowe rezultaty badań w zakresie zad. 2. zebrano w prezentacjach konferencyjnych i w publikacjach na temat uwarunkowań technicznych splątaniowych układów QKD w częściach dotyczących charakterystyk źródeł splątanych fotonów, a także pośrednio w zakresie ogólnych parametrów transmisyjnych.

Zadanie 3. Zbadanie dekoherencji nośników informacji kwantowej w różnych rodzajach kanałów kwantowych w układach kryptografii kwantowej bezsplątaniowej i splątaniowej.

W zadaniu prowadzono badania dotyczące dekoherencji kanałów kwantowych (tj. nieklasycznego szumu kwantowego, w opisie mechaniki kwantowej polegającego na splątywaniu się stopni swobody kodujących informację układów kwantowych ze stopniami swobody otoczenia) w bezsplątaniowych i splątaniowych układach kryptografii kwantowej. Badania obejmowały eksperymentalne testowanie parametrów dekoherencyjnych (pośrednio poprzez wydajnościowe parametryzowanie detekcyjne pojedynczych stanów kwantowych) dla różnych konfiguracji kanałów kwantowych. W toku badań zgodnie z założeniem dokonywano analizy maksymalnych eksperymentalnie osiągalnych zasięgów kanałów kwantowych w różnych typach światłowodów oraz w konfiguracji teleskopowej przy wykorzystaniu jako kanału kwantowego wolnej wiązki laserowej, m.in. w funkcji rosnących częstości transmisyjnych nośników i efektywnej szybkości generowania klucza. Badania prowadzone były w oparciu o 4 prototypy układów optyki kwantowej (w tym 2 bezsplątaniowe – kodujące informację kwantową w stanach przesunięć fazowych w układach interferometrycznych – oraz 2 splątaniowe, kodujące qubity na stanach polaryzacyjnych) oparte na platformach badawczo-rozwojowych QKD. Prototypy układów splątaniowych w toku badań były też konfigurowane jako bezsplątaniowe (w

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

takim przypadku kodując stany qubitów na polaryzacjach fotonów, a nie na przesunięciach fazowych jak w 2 pozostałych prototypach opartych na bezsplątaniowych platformach B+R QKD). Dla oceny własności dekoherencyjnych badano parametry wydajnościowe zaimplementowanych procedur modelowego stosu protokołu QKD – w tym warstw przesiewania klucza i destylacji klucza, procedur uzgadniania klucza (rekoncyliacji) oraz procedur wzmacniania prywatności (amplifikacji prywatności), a także właściwych procedur szyfrowania, zestawiając parametry wydajnościowe z badanymi konfiguracjami kanałów kwantowych. Zgodnie z założeniami prowadzono badania dla konfiguracji splątaniowych i bezsplątaniowych układów polaryzacyjnych w zakresach odległościowych do 10 km w światłowodach (w przypadku wolnej wiązki w optycznej konfiguracji teleskopowej na odległościach do 500 m) oraz dla układów bezsplątaniowych na odległościach do 50 km. W badaniach używano oprogramowania do specjalistycznej analizy danych badawczych (które wytworzone w modelu otwartego źródła zostało udostępnione na platformie internetowej projektu http://seqre.net). Zbadano szczegółowe charakterystyki parametrów dot. efektywnych zasięgów transmisji uwarunkowanych przez dekoherencję i ogólny zanik sygnału (dekoherencję amplitudową) w zależności od różnych ośrodków implementujących kanał kwantowy.

W toku badań zmierzono szczegółowe charakterystyki dekoherencyjne ośrodków kanałów kwantowych w postaci depolaryzacji (układy bezsplątaniowe i splątaniowe kodujące informację kwantową na polaryzacjach fotonów) oraz defazowania (układy bezsplątaniowe kodujące qubity informacji kwantowej na przesunięciach fazowych w konfiguracjach interferometrycznych). Wyniki badań pozwoliły na określenie ograniczeń dekoherencyjnych dla odległości realizacji procedur QKD w reżimach polaryzacyjnym i fazowym optyki kwantowej w protokołach opartych na splątaniu oraz w protokołach bezsplątaniowych. Dekoherencja polegająca na depolaryzacji (dwójłomność ośrodków optycznych w światłowodach) okazała się znacznie silniejsza niż dekoherencja fazowa dla przesunięć fazowych fotonów propagujących się w różnych ramionach optycznych interferometrów. Powoduje to, że układy splątaniowe i bezsplątaniowe oparte na polaryzacyjnych stopniach swobody stanowią mniej odporną technologię na zakłócenia kwantowe w kanałach optycznych niż bezsplątaniowe układy kodujące informację kwantową na przesunięciach fazowych (przy czym te ostatnie z kolei muszą być silnie tłumione co prowadzi do problemów z widzialnością sygnału, tj. dekoherencją amplitudową, raczej niż z dekoherencją fazową, tj. hybrydyzacyjnymi procesami splątaniowymi). Szczegółowe wyniki badań w zakresie dekoherencji kanałów kwantowych zebrano w publikacjach i prezentacjach konferencyjnych a ich adekwatnych zakresach. Badania te były także rozwinięte w szerszym zakresie w ramach zadania 5. (tj. w zakresie uwarunkowań topologicznych konfiguracji układów kryptografii kwantowej bezsplątaniowej i splątaniowej do zastosowań w rzeczywistych środowiskach sieciowych, których głównym aspektem był wpływ na dekoherencję elementów topologii łączy kwantowych, tj. w szczególności infrastruktur połączeniowych i spawów światłowodowych stanowiących nieodłączny element metropolitalnych sieci optycznych).

Zadanie 4. Zbadanie technicznych uwarunkowań detekcji nośników informacji kwantowej w układach kryptografii kwantowej bezsplątaniowej i splątaniowej.

W zadaniu realizowano badania w zakresie charakterystyk detektorów pojedynczych fotonów oraz związanych z nimi parametrów osiągalnych szybkości generowania klucza i poziomu błędów w transmisji QKD - QBER (determinowanych także przez charakterystyki źródeł oraz dekoherencji w kanałach kwantowych badanych szczegółowo w zadaniach 1.-3.). W ramach zadania analizowano graniczne parametry czułościowe i niezawodnościowe detekcji pojedynczych fotonów kodujących

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

qubity informacji kwantowej w celu realizacji protokołów QKD, obejmujące również tzw. ślepe zliczenia. Do problemów funkcjonowania detektorów jednofotonowych należą przekłamania detekcyjne ujemne i dodatnie (tj. odpowiednio niezarejestrowanie fotonu mimo jego obecności oraz fałszywe zarejestrowanie fotonu mimo faktycznego braku jego obecności – co jest możliwe w półprzewodnikowej technologii diód lawinowych, które ze względu na swoją ekstremalnie wysoką czułość, mogą przypadkowo poddać amplifikacji również sygnał pochodzący z dynamiki samej struktury półprzewodnikowej, a nie promieniowania e-m z zewnątrz w postaci padającego fotonu). Badania prowadzono w ramach platform B+R prototypowych układów QKD w architekturach detekcyjnych stanów polaryzacyjnych i fazowych przy różnicowanych parametrach odpowiadających rzeczywistym konfiguracjom układów komponentów optyki kwantowej dla zastosowania procedur QKD w środowiskach laboratoryjnych i w toku pilotażowych wdrożeń w sieciach metropolitalnych. Dzięki komponentom detekcyjnym intensywnego oświetlenia detektorów jednofotonowych (diód lawinowych) zweryfikowano możliwość skutecznego przeciwdziałania atakom oślepiającym (tzw. blinding attacks, które prowadzą do zademonstrowanego przez zespół norwesko-niemiecki przejęcia kontroli nad detektorem jednofotonowym i efektywnie pełną kontrolę sterowania fałszymi detekcjami co poza klasą ataków PNS stanowi kolejny pod względem istotności problem implementacyjny układów bezsplątaniowej QKD). W toku badań przeprowadzono charakterystyki statystyczne właściwych zliczeń detekcyjnych, tj. rejestracji pojedynczych fotonów, braków detekcji oraz tzw. ślepych zliczeń i przeprowadzono analizy związane z ogólnymi charakterystykami wyższych warstw logicznych protokołów QKD (w tym w zakresie parametrów osiągalnych szybkości generowania klucza oraz poziomu błędów w transmisji QBER). W tym obszarze badań koncentrowano się na wpływie niezawodności detektorów na parametry techniczne implementacji obu reżimów QKD – bezsplątaniowego i splątaniowego (w tym na przebieg procedur przesiewania, destylacji, uzgadniania i rekoncyliacji klucza oraz procedur amplifikacji prywatności, również w odniesieniu do parametrów niezawodnościowych oraz wydajnościowych w charakterystyce poziomu błędów QBER, maksymalnego zasięgu efektywnej transmisji klucza kwantowego oraz szybkości generowania klucza). Istotnym obszarem eksperymentalnych prac badawczych w zakresie protokołów splątaniowych i bezsplątaniowych opartych na układzie optyki kwantowej dla qubitów polaryzacyjnych była synchronizacja okien czasowych pomiarów (w protokołach bezsplątaniowych opartych na przesunięciach fazowych problematyka synchronizacji jest z definicji częścią układu interferometrycznego). W obszarze wykorzystania polaryzacji fotonów do kodowania informacji w kanale kwantowym dla protokołów QKD wykorzystujących lub niewykorzystujących splątanie kwantowe było ustalenie zgodnych okien czasowych pomiarów, związane z bardzo dokładnym znakowaniem czasowym impulsów laserowych przechodzących przez kryształ nieliniowy w procedurze spontanicznej parametrycznej konwersji w dół (SPDC) w krzysztale BBO. Warunkiem koniecznym dla implementacji w warstwie logicznej protokołów splątaniowych i bezsplątaniowych jest identyfikacja obu odpowiednich części składowych par splątanych fotonów, które mogą być zrzutowane do stanów niesplątanych po natychmiastowym pomiarze jednego z fotonów i transmisji drugiego fotonu w stanie już niesplątanym, lub zachowane w swoim wspólnym stanie splątanym na czas całej transmisji i zrzutowane dopiero po jej realizacji. W prototypowym układzie optyki kwantowej dla stanów polaryzacyjnych duża część prac laboratoryjnych wiązała się z badaniami odpowiednich metod i systemów synchronizujących poprzez dokładne znakowanie czasowe. Szczegółowe wyniki badań w zakresie zad. 5. zebrano w prezentacjach konferencyjnych i w publikacjach w ich częściach na temat uwarunkowań technicznych dla detekcji nośników informacji

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

kwantowej w układach QKD bezsplątaniowych i splątaniowych, pośrednio determinujących charakterystki transmisyjne procedur QKD.

Zadanie 5. Zbadanie uwarunkowań topologicznych konfiguracji układów kryptografii kwantowej bezsplątaniowej i splątaniowej do zastosowań w rzeczywistych środowiskach sieciowych.

W zadaniu prowadzono badania nad uwarunkowaniami topologicznymi dla układów kryptografii kwantowej splątaniowej i bezsplątaniowej w celu zastosowań w ramach wdrożeń w rzeczywistych środowiskach sieciowych. Ze względu na fundamentalne dla informacji kwantowej twierdzenie o zakazie klonowania stanów informacji kwantowej ważnym ograniczeniem topologicznym na poziomie architektury pojedynczego układu QKD jest topologia P2P (czyli punkt-do-punktu). Pomimo to, możliwe są rozbudowane topologie wielo-węzłowe (uogólnienia topologii gwiazdy i grafów wielowęzłowych) przy zachowaniu pewnych założeń koncepcyjnych (np. zaufanie poszczególnych węzłów). Badania w tym obszarze koncentrowały się na modelowaniu najprostszej topologii gwiazdy (obejmującej 3 węzły, z jednym węzłem w środku) w ramach trzech lokalizacji wirtualnych, a następnie pilotażowo wdrożanych w rzeczywistym środowisku infrastruktur telekomunikacyjnych światłowodowej sieci metropolitalnej. W ramach zadania w zakresie badań dla rozszerzenia uwarunkowań topologicznych QKD poza model P2P prowadzono też badania w zakresie możliwości opracowania oprogramowania standaryzującego protokoły komunikacji kwantowej rozszerzającej topologię P2P. Badania obejmowały łącza tunelowe i systemy zarządzania kluczem z procedury kwantowej dystrybucji, tak aby fizyczną warstwę P2P (fundamentalnie uwarunkowaną przez prawa mechaniki kwantowej) można było na poziomie warstw logicznych uogólnić do topologii gwiazdy, a także wielowęzłowej topologii sieciowej (w której działa sieć Internet). Badania koncepcyjne dotyczące wymagań funkcjonalnych dla takiego oprogramowania stały się podstawą dla prowadzonej w toku prac rozwojowych implementacji programistycznych w zadaniu 7.). W szczególności w tym obszarze ważną częścią prac badawczych stanowiła standaryzacja i integracja interfejsowa na poziomie warstw logicznych protokołów tunelowych (dla wirtualnych sieci prywatnych VPN) oraz aplikacji zarządzania kluczem różnych systemów fizycznej warstwy kryptografii kwantowej przeprowadzających w oparcia o prawa mechaniki kwantowej dystrybucję klucza QKD, w tym systemów QKD bezsplątaniowych i splątaniowych. Problematyka praktycznej integracji kryptografii kwantowej z informatycznymi sieciami klasycznymi była przedmiotem badań w zakresie możliwości integracji logicznej w modelu ISO/OSI w ramach zaprojektowania interfejsowych warstw współpracy z protokołami sieci internetowych w tym w szczególności protokołami warstwy sieciowej i stosu protokołowego IP/IPSec, służącego zabezpieczeniu wyższych protokołów warstwy transportowej w Internecie, np. protokołów TCP i UDP oraz przeróżnych protokołów warstwy aplikacyjnej. Badania te po rozpoznaniu możliwości optymalnego włączenia procedury kwantowej dystrybucji klucza QKD, tj. kryptografii kwantowej do zabezpieczenia komunikacji internetowej zakończyły się ustaleniem koncepcji protokołowego oprogramowania interfejsowego dla wyższych warstw komunikacji w modelu ISO/OSI (w tym np. warstwy IKE w protokole IPSec) czyniąc z klasycznego klucza (losowego ciągu bitowego) teoretycznie bezwarunkowo bezpiecznie dystrybuowanego w kwantowej warstwie fizycznej QKD, współdzielony zasób dla wyższych warstw protokołowych komunikacji lub bezpośrednio dla programów z warstwy aplikacji modelu ISO/OSI (oprogramowanie interfejsowe kwantowej dystrybucji klucza QKD wraz z systemami tunelowymi i systemami zarządzania kluczem zostało następnie zaimplementowane w toku zadania 7. projektu). W warstwie fizycznej protokołów bardzo istotnym problemem w zakresie topologii łączy są uwarunkowania rzeczywistej infrastruktury metropolitalnej sieci światłowodowej. Metropolitalna infrastruktura optyczna dla sieciowych

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

połączeń szkieletowych jest determinowana topologicznie rozkładem miejskich kanałów telekomunikacyjnych. Tzw. ciemne włókna (wolne od transmisji włókna światłowodów, pozostające w dyspozycji do komunikacji bez konieczności stosowania multipleksingu, który w przypadku kwantowym stanowi istotny problem koncepcyjno-technologiczny) łączące nawet nieodległe lokalizacje fizycznie dzielące standardowy telekomunikacyjny światłowód z wieloma równoległymi włóknami (tworzącymi zarys szkieletowy topologii P2P dla zastosowań kwantowej dystrybucji klucza QKD) są rozdzielone ciągami połączeniowych spawów termicznych na rozwidleniach kanalizacyjnych. Pomimo zachowania fundamentalnej topologii P2P zestawianie ciemnych włókien z różnych fizycznie przewodów światłowodowych wiąże się z koniecznością wprowadzania światłowodowych spawów termicznych (zespoleń pojedynczych włókien światłowodów zachowujących możliwie niezmienione parametry transmisyjne dla światła). Zarówno standardowe złącza optyczne jak i spawy termiczne stanowią istotne dodatkowe do dwójłomności światłowodowej źródło dekoherencji kwantowej i zaniku koherentnego sygnału kwantowego. Rola tego procesu jest znacznie bardziej istotna dla koherentnych i silnie tłumionych sygnałów kwantowych niż dla optycznych sygnałów klasycznych, dla których dekoherencja, np. depolaryzacja, jest tylko w niewielkim stopniu nieistotna, ze względu na brak istotności co do koherencji kwantowej sygnału oraz znacznie większe intensywności). Dekoherencja na złączach i spawach obecnych w architekturze rzeczywistych światłowodowych sieci metropolitalnych, przy topologii P2P, a następnie przy topologii gwiazdy (badana najpierw w toku symulacji laboratoryjnych, a następnie w toku pilotażowych wdrożeń w infrastrukturach telekomunikacyjnych) powoduje zwiększone parametry błędów (QBER), utrudniające lub uniemożliwiające implementację pełnego zakresu warstw protokołowych QKD w praktycznych zastosowaniach w przypadku stanów polaryzacyjnych (głównie związanych z optyczną siecią szkieletową łączącą w rozkładzie metropolitalnym dwie stosunkowo odległe - o co najmniej kilka km – lokalizacje; dla odległości rzędu 5 km, w sieci metropolitalnej występuje nawet kilkanaście spawów termicznych włókien). Wyniki badań zestawiono w publikacjach i prezentacjach konferencyjnych omawiających perspektywy komercyjne dla obu rozwiązań o odmiennym charakterze technicznym, tj. systemów kwantowej dystrybucji klucza QKD niewykorzystujących i wykorzystujących splątanie kwantowe w rzeczywistych środowiskach wdrożeniowych (w szczególności rezultatem badań są parametry techniczne efektywnego zasięgu eksperymentalnych układów kryptografii kwantowej kodujących stany kwantowe na polaryzacji i przesunięciach fazowych, warunkowane dopuszczalnym poziomem błędów QBER, a także zbadanie wpływu topologicznych uwarunkowań infrastruktur sieciowych, pośrednio poprzez dekoherencję, na ograniczenia szybkości dystrybucji klucza).

Zadanie 6. Zbadanie problemu uwierzytelnienia sesji kryptografii kwantowej układów bezsplątaniowych i splątaniowych.

W zadaniu prowadzono prace badawcze w zakresie problematyki uwierzytelnienia sesji kryptografii kwantowej. Badania realizowane były zarówno w zakresie koncepcyjno-protokołowym jak i eksperymentalnym. Problem uwierzytelnienia (zapewnienia autentyczności stron komunikacji) ma kluczowe znaczenie dla bezpieczeństwa kryptosystemu. Sytuacja taka ma miejsce nie tylko dla klasycznych protokołów kryptograficznych, ale także dla procedury dystrybucji klucza kwantowego QKD. Aby zapewnić teoretycznie bezwarunkowe bezpieczeństwo kryptosystemu QKD, należy rozwiązać problem wykluczenia abstrakcyjnej klasy ataków polegających na impersonifikacji stron komunikacji wobec siebie. Ataki typu *man-in-the-middle* mogą być wykluczone tylko na podstawie protokołów uwierzytelnienia, które pozwolą zweryfikować obu stronom komunikacji, że ich partner jest autentyczny. Brak uwierzytelnienia może spowodować nieświadomą wymianę klucza

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

kwantowego z adwersarzem (przy fałszywym przekonaniu, że dystrybucja klucza ma miejsce z uprawnioną stroną komunikacji). Nawet jeśli wymiana ta ma charakter teoretycznie bezwarunkowo bezpieczny (dzięki prawom mechaniki kwantowej w protokole QKD), to dochodzi do niej z adwersarzem, z którym (w sposób bezwarunkowo bezpieczny) współdzielony jest klucz kwantowy. Taka sytuacja oznacza oczywiście całkowitą kompromitację kryptosystemu, ponieważ adwersarz, może impersonifikować obie strony komunikacji względem ich partnerów, będąc nieujawnionych pośrednikiem komunikacji, tj. mając możliwość naruszenia trzech podstawowych paradygmatów kryptograficznych, tj. poufności, wiarygodności i integralności komunikacji (ma on możliwość zarówno niewykrytego podsłuchu komunikacji jak i jej dowolnego preparowania). Sytuacja taka jest możliwa tylko w przypadku przejęcia przez stronę podsłuchującą obu kanałów komunikacji (klasycznego i kwantowego), ale w ogólności całkowicie dopuszczalna. Jedynym przeciwdziałaniem klasie ataków *man-in-the-middle* jest procedura uwierzytelnienia, która aby zachować bezwarunkowy poziom bezpieczeństwa protokołu QKD, sama również musi być bezwarunkowa. Fundamentalnym aspektem procedury uwierzytelniania jest współdzielenie pomiędzy stronami komunikacji wstępnego sekretu (którego rolę może pełnić symetryczny klucz kryptograficzny) – w tym kontekście można zaznaczyć, że protokoły QKD (dystrybucji klucza kwantowego, *quantum key distribution*), często nazywane są także protokołami QKE (rozszerzania klucza kwantowego, *quantum key expansion*), w których część wymienianego klucza symetrycznego jest na bieżąco wykorzystywana do podtrzymania procedur uwierzytelniania. W toku badań prowadzono analizę oraz ocenę teoretycznych i praktycznych aspektów skutecznego przeciwdziałania względem klas ataków opierających się na problemie uwierzytelnienia przy założeniu przechwycenia kanału kwantowego i klasycznego w celu próby impersonifikacji jednej ze stron komunikacji. Analizy badawcze ukierunkowane na protokoły uwierzytelnienia gwarantujące zachowanie teoretycznie bezwarunkowego poziomu bezpieczeństwa (konieczne do podtrzymania takiej własności kryptograficznych systemów kryptografii kwantowej) uwzględniały wykorzystanie metod uwierzytelniających opartych na uniwersalnych klasach funkcji mieszających Wegmana-Cartera oraz bardziej zaawansowanych metod opartych na splątaniu kwantowym, stanowiącym uprzednio współdzielony zasób (i w założeniu rozszerzany w toku procedury wymiany splątania w ramach splątaniowych protokołów kryptografii kwantowych). Szczegółowe rezultaty badań w zakresie zadania 5. zebrano w prezentacjach konferencyjnych i w publikacjach w częściach dotyczących problematyki uwierzytelniania kryptograficznego.

5. Opis przeprowadzonych prac rozwojowych

W projekcie zrealizowano następujące zadania w zakresie zaplanowanych prac rozwojowych:

Zadanie 7. Implementacja oprogramowania interfejsowego systemów kryptografii kwantowej.

W toku zadania zrealizowano implementacje programistyczne warstw protokołowo-interfejsowych dla prototypowych układów kryptografii kwantowej. Ważny obszar implementacji programistycznych stanowił zbiór interfejsowych skryptów kontrolujących układy QKD, umożliwiających przetwarzanie otrzymywanych danych parametrycznych z układów opto-elektronicznych w odpowiednie dane wyjściowe do dalszego przetwarzania i analizy. Przetworzone dane umożliwiają monitorowanie i analizę wybranych parametrów układu wyższej abstrakcji logicznej, np. parametr QBER kwantowego błędu, a predefiniowane karty kontrolne analizy statystycznej umożliwiają generowanie danych do przetwarzania statystycznego. Pakiet oprogramowania interfejsowego dla splątaniowego układu QKD

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

uwzględnia możliwości kontroli polaryzacji dla rekalibracji najistotniejszego parametru splątaniowego układu kwantowej dystrybucji klucza – koherencji parametru polaryzacji odplątanego fotonu podróżującego do docelowego punktu końcowego. W zadaniu zaimplementowano również oprogramowanie symulacyjne układów QKD splątaniowych i bezsplątaniowych, które miało zadania wspomagania prac badawczych oraz realizacji szkoleń wdrożeniowych i dydaktycznych. Kolejnym istotnym zakresem implementacyjnym oprogramowania interfejsowego były skrypty aplikacyjne sterowania kwantowymi generatorami liczb losowych QRNG (o krytycznym znaczeniu w warstwie fizycznej dla bezsplątaniowych układów QKD – w zakresie sterowania prawdziwie losowym wyborem baz pomiarowych – oraz o ważnym zastosowaniu w zakresie wyższych, logicznych protokołów QKD obu reżimów przy normalizacji klucza jako konieczne działanie wstępne przed procedurą rekoncyliacji klucza). Interfejsowe oprogramowanie sterowania QRNG dla systemów Linux umożliwia dostęp i kontrolę urządzenia sprzętowo generującego kwantowe ciągi losowe zapewniając warstwę interoperacyjności ze skryptami kontrolnymi układów QKD. Urządzenie QRNG jest generatorem liczb losowych, którego działanie oparte jest na prawach mechaniki kwantowej zapewniając tym samym pełną losowość wynikającą z fundamentalnych praw fizyki, które pozostają poza zasięgiem klasycznej informatyki (chaotyczne procesy losowe są w istocie w pełni opisane przez deterministyczne prawa mechaniki klasycznej i dlatego poprawnie określa się je jako pseudolosowe). Modele koncepcyjne i projekty oprogramowania w zakresie warstw protokołowych oraz interfejsowych były determinowane odpowiednio przez wyniki badań przemysłowych w toku realizacji zadań 1-3 oraz 5. W zadaniu 7. przeprowadzono implementację oprogramowania standaryzującego protokoły komunikacji kwantowej rozszerzającej topologię P2P (na podstawie prac badawczych z zadania 5.), ze szczególnym naciskiem na wyższe warstwy protokołowe, w których możliwa jest integracja protokołów układów kryptografii kwantowej QKD zarówno ze środowiskiem sieciowym (w modelu ISO/OSI) jak i w logicznej warstwie zarządzania kwantową dystrybucją klucza w topologii rozszerzającej model P2P z równoczesnym uwzględnieniem interoperacyjności różnych w zakresie koncepcyjnym i technologicznym układów bezsplątaniowych i splątaniowych QKD). Implementacja oprogramowania objęła opracowane teoretycznie i wstępnie zaprojektowane w toku badań przemysłowych protokoły tunelowe i systemy zarządzania kluczem z procedury jego kwantowej dystrybucji. W tym pierwszym zakresie oprogramowanie warstwy interfejsowej komunikacji miało postać warstwy tunelowej P2P umożliwiającej przesyłanie wiadomości i plików w zabezpieczonym kanale (i wytworzenie sieci VPN). Oprogramowanie tunelowe pozwala na kontrolę metod zabezpieczenia (symetryczne bądź asymetryczne) m.in. DES, RSA, AES, OTP, a także umożliwia wybór kluczy do szyfrowania, dystrybuowanych przez system QKD. Implementacja tych systemów pozwala w praktyce rozszerzyć topologię modelu P2P (uwarunkowaną przez prawa mechaniki kwantowej) do ogólniejszej topologii gwiazdy, a także wielowęzłowej topologii grafu, w której działa sieć Internet. Oprogramowanie interfejsowe integracji protokołów QKD z protokołami sieciowymi Internetu przetestowano w praktyce w toku pilotażowych metropolitalnych wdrożeń sieciowych obejmujących 3 lokalizacje w sieci. Implementacje programistyczne realizowane były w celu zapewnienia możliwości standaryzacji działania kwantowej dystrybucji klucza i jej integracji interfejsowej na poziomie warstw logicznych protokołów tunelowych (dla wirtualnych sieci prywatnych VPN) oraz aplikacji zarządzania kluczem różnych systemów fizycznej warstwy kryptografii kwantowej przeprowadzających w oparciu o prawa mechaniki kwantowej dystrybucję klucza QKD, w tym dla systemów QKD zarówno bezsplątaniowych jak i splątaniowych. Problematyka praktycznej integracji kryptografii kwantowej z informatycznymi sieciami klasycznymi była przedmiotem badań w zakresie możliwości integracji logicznej w modelu ISO/OSI w toku zadania 5., czego rezultatem było

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

zaprojektowanie interfejsowej warstwy współpracy z protokołami sieci internetowych w tym w szczególności protokołami warstwy sieciowej i stosu protokołowego IP/IPSec, służącego zabezpieczeniu wyższych protokołów warstwy transportowej w Internecie, np. protokołów TCP i UDP oraz przeróżnych protokołów warstwy aplikacyjnej. Warstwy te zostały zaimplementowane programistycznie właśnie w niniejszym zadaniu 7. Implementacje oparto na wynikach badań rozpoznających możliwości optymalnego włączenia procedury kwantowej dystrybucji klucza QKD do zabezpieczenia komunikacji internetowej (w wyniku których powstały wstępne koncepcje protokołowego oprogramowania interfejsowego dla wyższych warstw komunikacji modelu ISO/OSI, w tym np. możliwe do wdrożenia jako warstwa IKE w protokole IPSec) czyniąc z klasycznego klucza (losowego ciągu bitowego), który został teoretycznie w pełni bezwarunkowo bezpiecznie rozdystrybuowany w kwantowej warstwie fizycznej QKD, jako współdzielony zasób dla wyższych warstw protokołowych komunikacji i bezpośrednio dla konkretnych programów z warstwy aplikacji modelu ISO/OSI. W tym kontekście w toku zadania zaimplementowano oprócz oprogramowania interfejsowego kwantowej dystrybucji klucza QKD wraz z systemem tunelowym również system zarządzania kluczem jako współdzielonym zasobem dla wyższych warstw ISO/OSI. System zarządzania kluczem umożliwia wymagany do rzeczywistych zastosowań strumieniowych wzrost szybkości szyfrowania kryptograficznego w protokołach hybrydowych (opartych na szyfrach AES i 3DES, które jako kluczy używają standardowych krótkich ciągów losowych w przeciwieństwie do pełnych rozwiązań OTP bazujących na kluczach o długościach wiadomości). W toku pilotażowych wdrożeń prototypowych układów kryptografii kwantowej splątaniowej i bezsplątaniowej w sieciach metropolitalnych zademonstrowano interoperacyjną dla różnych technologii warstwy fizycznej QKD wirtualną sieć prywatną VPN kryptograficznie zabezpieczoną kryptografią kwantową w trybie OTP, tj. teoretycznie bezwarunkowego poziomu bezpieczeństwa komunikacji. Stanowiąca podstawę tego wdrożenia w warstwie logicznej protokołowo-interfejsowa implementacja programistyczna stanowi płaszczyznę wyjściową dla praktycznych zastosowań komercjalizowanej kryptografii kwantowej. Wytworzone oprogramowanie zgodnie z założeniami zostało udostępnione w modelu otwartego źródła na platformie internetowej projektu http://seqre.net.

Zadanie 8. Opracowanie dokumentacji technicznej w zakresie instalacji i konfiguracji eksperymentalnych układów kryptografii kwantowej splątaniowej i bezsplątaniowej.

W ramach prac rozwojowych realizowanych w zadaniu 8 zostały opracowane dwie techniczne dokumentacje opisujące strukturę techniczną, komponenty składowe oraz konfigurację i instalację w optymalnym zakresie prototypowych układów kryptografii kwantowej bezsplątaniowej i splątaniowej. Dokumentacje techniczne zostały oparte na wynikach realizacji wszystkich zadań zaplanowanych w projekcie i opisanych powyżej w ramach badań przemysłowych i prac rozwojowych. Dokumentacje techniczne zawierają szczegółowe opisy techniczne komponentów opto-elektronicznych układów QKD oraz opisy instalacji i konfiguracji układów, mając na celu umożliwienie zaangażowym przy uruchomieniu linii produkcyjnych systemów QKD kadrom inżynieryjnym i technicznym przeprowadzenie realizacji przyszłych prac wdrożeniowych kryptografii kwantowej w środowisku komercyjnym, w tym przygotowanie rynkowej oferty produktowej. Dokumentacje techniczne prototypowych układów QKD udostępniono na platformie internetowej komercjalizacji kryptografii kwantowej http://seqre.net.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

6. Wyniki z przeprowadzonych badań przemysłowych i prac rozwojowych – uzasadnienie osiągnięcia założeń zawartych we wniosku i biznesplanie

W ramach przeprowadzonych badań przemysłowych i prac rozwojowych, których wyniki dokładnie opisano w punkcie E. udało się zrealizować wszystkie założenia projektowe. W szczególności zbadano techniczne uwarunkowania źródeł zarówno niesplątanych jak i splątanych nośników kwantowych i możliwości kodowania na nich informacji w układach QKD odpowiednio bezsplątaniowych oraz splątaniowych. Zbadano także zjawiska dekoherencyjne nośników informacji kwantowej w różnych rodzajach kanałów kwantowych w układach kryptografii kwantowej bezsplątaniowej i splątaniowej zgodnie z założeniami projektowymi. Przebadano techniczne uwarunkowania detekcji nośników informacji kwantowej w układach kryptografii kwantowej bezsplątaniowej i splątaniowej oraz zbadano uwarunkowania możliwych topologicznych konfiguracji układów kryptografii kwantowej (zarówno bezsplątaniowej i splątaniowej) do zastosowań w rzeczywistych środowiskach sieciowych (w ramach których dokonano pilatożowych wdrożeń, stanowiących demonstratory technologii). Zgodnie z założeniami projektowymi zbadano ponadto problem uwierzytelnienia sesji kryptografii kwantowej układów bezsplątaniowych i splątaniowych w reżimie protokołów klasycznych (Wegman-Carter) oraz kwantowych opartych na splątaniu. Wszystkie uzyskane wyniki badań przemysłowych, zgodnie z deklaracjami zawartymi we wniosku projektowym szeroko upowszechniono na konferencjach międzynarodowych i w publikacjach w specjalistycznych czasopismach naukowo-technicznych i wydawnictwach (w tym także udostępniono na platformie internetowej projektu http://seqre.net). Dopełniając założeń projektowych w zakresie prac rozwojowych z powodzeniem zrealizowano prace obejmujące implementację oprogramowania protokołowo-interfejsowego prototypowych systemów kryptografii kwantowej oraz opracowano dokumentacje techniczne w zakresie instalacji i konfiguracji eksperymentalnych układów QKD. Zarówno implementacje programistyczne (w modelu otwartego źródła) jak i dokumentacje techniczne również udostępniono na platformie internetowej projektu http://seqre.net, dopełniając deklaracji o ich upowszechnieniu). W toku realizacji badań przemysłowych oraz towarzyszących im prac rozwojowych potwierdzono możliwości implementacji technologicznej w obecnym stanie rozwoju techniki komercyjnych układów QKD bezsplątaniowych i splątaniowych oraz wypracowano nowe koncepcje protokołowe i techniczne, obecnie znajdujące się w fazie zapewniania im ochrony własności intelektualnej poprzez międzynarodowe procedury patentowe (formalno-prawnę realizację których, wspiera program PatentPlus). Produkcję komercyjnych układów opartych o wyniki badań projektu realizator planuje w ramach kolejnego, wdrożeniowego etapu komercjalizacji QKD, prowadząc jednocześnie działania rynkowe mające na celu pozyskanie pierwszych zamówień rynkowych w kraju i za granicą.

7. Analiza SWOT I Etapu projektu (Mocne strony, Słabe strony, Szanse, Zagrożenia)

Analizę SWOT dla I Etapu projektu (projekt obejmujący prace B+R w ramach działania 1.4 PO IG) przygotowano w odniesieniu do 2 kierunków prac badawczo-rozwojowych w zakresie przygotowania do komercjalizacji bezsplątaniowych oraz splątaniowych układów kryptografii kwantowej. Ze względu

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

na różnice mocnych i słabych stron obu technologii analiza SWOT została dla obu tych aspektów odpowiednio rozdzielona (w odniesieniu do układów bezsplątaniowych i splątaniowych QKD).

Mocne strony

- **Bezsplątaniowe układy QKD**
  - Stabilna i odporna na zakłócenia zewnętrzne interferencja fazowa jako stan kwantowy qubitu
  - Wysokie parametry zasięgowe, umożliwiające implementacje metropolitalne (niski poziom dekoherencji kwantowej z uwagi na nieistotność dla kodowania fazowego dwójłomności ośrodków transmisyjnych prowadzących do depolaryzacji w toku defazowania stanu fotonu)
  - Wysokie parametry transmisyjne, umożliwiające zabezpieczenie szerszych strumieni danych (przede wszystkim w trybie OTP jako jedynym gwarantującym teoretycznie bezwarunkowe bezpieczeństwo – w trybie hybrydowym symetrycznym przy stosowaniu kluczy krótszych od wiadomości przy połączeniu z klasycznym kryptosystemem jest to mniej istotna przewaga)
  - Dzięki dostępności wysoce zintegrowanych komponentów optyki kwantowej układy mają kompaktowe rozmiary i są zgodne ze standaryzacją rozmiarową sprzętu sieciowego co ułatwia przyszłe wdrożenia i dodatkowo wpływa pozytywnie na stabilność i bezawaryjność
  - Przy kodowaniu fazowym w układzie interferometrycznym architektura układu jest optymalna dla topologii gwiazdy (stacje odbiorcze Alice o niskiej złożoności i relatywnie niskich kosztach)

- **Splątaniowe układy QKD**
  - Dzięki unikalnemu wyróżnieniu pojedynczych stanów kwantowych poprzez splątanie kwantowe par fotonów, układy QKD splątaniowe gwarantują odporność na ataki typu PNS (nie zachodzi potrzeba tłumienia impulsów laserowych dla zapewnienia niskiej statystyki liczby fotonów na impuls – w przypadku układów QKD splątaniowych w wiązce laserowej w danym oknie czasowym znajduje się tylko jeden, unikalny stan kwantowy odpowiadający poprzez korelację partnerowi z pary)
  - Dzięki wyeliminowaniu konieczności silnego tłumienia impulsów laserowych splątaniowe układy QKD są bardziej perspektywiczne do zastosowań satelitarnych (komunikacja teleskopowa wiązką laserową w atmosferze lub w przestrzeni kosmicznej, gdzie występuje niska depolaryzacja, co dodatkowo wspiera adekwatność tego rodzaju układów do satelitarnych zastosowań komunikacyjnych)
  - Fundamentalnie nieklasyczna nielokalność splątania kwantowego, który stanowi podstawę protokołów QKD splątaniowych otwiera szerokie możliwości dla nowych zastosowań koncepcyjno-protokołowych w obszarze kryptograficznym i ogólniej komunikacyjnym (dotyczy to pojęć takich jak teleportacja kwantowa informacji, czy QSDC – tj. bezpośrednia bezpieczna komunikacja kwantowa bez konieczności dystrybucji klucza w sposób nielokalny względem kanału komunikacyjnego – informacja nie jest nim komunikowana lokalnie, a ponadto w przyszłości istotne obszary kryptograficzne dotyczące kodowania informacji kwantowej dla

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

zabezpieczenia komputerów kwantowych); w tym kontekście rozwój technologii splątaniowej komunikacji kwantowej otwiera znacznie szersze pole zastosowań niż bezsplątaniowej

Słabe strony

- **Bezsplątaniowe układy QKD**
  - Brak fundamentalnej ochrony przed atakami typu PNS (ochrona taka możliwa jest tylko w reżimie splątania kwantowego, które gwarantuje, że określony stan kwantowy dotyczy tylko jednego transmitowanego fotonu – konkretnie tego który znajduje się w parze ze zmierzonym fotonem, fundamentalnie musi być unikalny)
  - Ze względu na wykorzystanie silnego tłumienia laserowego (dla zachowania probabilistycznej dystrybucji liczby fotonów na impuls mniejszej lub równej jednemu fotonowi, dla zachowania efektywnej odporności na ataki typu PNS) technologia QKD bezsplątaniowa jest mniej perspektywiczna dla zastosowań komunikacji wiązką laserową w przestrzeni (zastosowania satelitarne)
  - W układzie przyjęto implementacje fazowe qubitów (kodowanie informacji kwantowej na przesunięciach fazowych w układach interferometrycznych, które mogą w pewnych konfiguracjach być niekoherentne i demonstrować właściwości klasyczne)
  - Technologia bezsplątaniowa oparta na przesunięciach fazowych fotonów (stopnie swobody stosunkowo odporne na dekoherencję w kanałach światłowodowych) wymaga architektury dróg optycznych interferometru Macha-Zehndera, co również komplikuje zastosowania praktyczne w komunikacji satelitarnej

- **Splątaniowe układy QKD**
  - Stosunkowo silnie (relatywnie do stopni swobody stanów przesunięć fazowych) podatne na dekoherencję polaryzacyjne stopnie swobody (efekty depolaryzacyjne w ośrodkach dwójłomnych) jako stany qubitów informacji kwantowej
  - W związku z powyższym niższe od bezsplątaniowych parametry zasięgowe, umożliwiające implementacje metropolitalne w ograniczonej skali (do kilku kilometrów przy stabilnej pracy)
  - Implementacja technologiczna ze względu na mniejszy poziom integracji układów produkcji splątania kwantowego podatna na zakłócenia zewnętrzne (głównie mechaniczne) i w związku z tym mniej stabilna od bezsplątaniowej (konieczne rekalibracje wiązek optycznych, korekta dryfu wiązki laserowej, korekta depolaryzacji światłowodowej)
  - Niższy poziom zintegrowania komponentów optyki kwantowej w porównaniu z układami bezsplątaniowymi, co prowadzi do większych gabarytów i niski poziom zgodność ze standardami (brak integracji procesu SPDC determinujący konieczność makroskopowej implementacji drogi optycznej stanów kwantowych, która jest podatna na dekalibrację ze względu na czynniki mechaniczne i materiałowe)
  - Architektura układu mniej optymalna dla topologii gwiazdy (konieczność obecności kosztownego modułu detekcyjnego w stacjach odbiorczych Boba – wysokie koszty)

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

Szanse

- Oczekiwany przełom w informatyce kwantowej polegający na budownie komputera kwantowego spowoduje rewolucję informatyczną oraz nagły, lawinowy wzrost zapotrzebowania na kryptografię kwantową, a także pociągnie za sobą nieporównanie bardziej intensywny rozwój technologiczno-przemysłowy w zakresie produkcji nowych generacji komponentów optyki kwantowej (prowadząc do dalszej miniaturyzacji układów)
- Postęp w zakresie miniaturyzacji polaryzacyjnych i fazowych komponentów optyki kwantowej w układach chipowych, a także postęp w zakresie interfejsów elektro-optycznych w reżimie sprzężenia światło-materia (w tym stanów polarytonów), może otworzyć zupełnie nowy obszar technologiczny dla integracji kwantowych układów optycznych i klasycznych układów elektronicznych (jest to obecnie bardzo silnie rozwijany obszar technologiczny i z całą pewnością będzie mocno warunkował rozwój i miniaturyzację kryptografii kwantowej)
- Przy zachowaniu parametrów operacyjnych dalsze miniaturyzacja układów wymaga rozwiązania problemu generacji splątania w układzie zintegrowanym (splątanie w chipie, na świecie prowadzone są badania w tym zakresie, postęp w nich umożliwi zastosowanie bardziej zintegrowanych komponentów optyki kwantowej dla układów splątaniowych)
- Postęp w zakresie diód lawinowych (detektory pojedynczych fotonów) w układach chipowych – obecnie dla kryptografii bezsplątaniowej opartej na kodowaniu fazowym problematyczne są kwestie detekcyjne pojedynczych fotonów w silnie tłumionych impulsach laserowych – w tym obszarze oczekuje się silnego rozwoju technologicznego (w zakresie miniaturyzacji i integracji chipowej półprzewodnikowych diód lawinowych)
- W zakresie algorytmiki klasycznej ewentualny postęp w obszarze teorii złożoności obliczeniowej może spowodować odkrycie nowych klasycznych algorytmów redukujących trudną (i przez to niepraktyczną do implementacji, co stanowi fundament bezpieczeństwa asymetrycznej kryptografii klasycznej) złożoność obliczeniową określonych problemów matematycznych (np. znajdowania dyskretnego logarytmu, czy faktoryzacji liczb na czynniki pierwsze) – w takiej sytuacji, nawet bez skalowalnego, uniwersalnego komputera kwantowego nastąpi lawinowy wzrost zapotrzebowania na kryptografię kwantową

Zagrożenia

- Dekoherencja kwantowa może okazać się zjawiskiem, którego nie da się ani uniknąć, ani skorygować procedurami korekty błędów kwantowych – w takim przypadku dekoherencja byłaby elementem ogólniejszych praw natury stojących na drodze integracji koherentnego przetwarzania informacji kwantowej z przetwarzaniem informacji klasycznej (co w pewnym stopniu odnosi się do problemu zrozumienia granicy między światem kwantowym, a klasycznym, co do tej pory stanowi fundamentalny niewyjaśniony problem w fizyce – do udzielenia odpowiedzi na to pytanie konieczne jest skonstruowanie skalowalnego i uniwersalnego komputera kwantowego albo opracowanie kwantowej teorii grawitacji, co leży w obszarze badań podstawowych i od wielu lat jest bez powodzenia realizowane)
- W powiązaniu z poprzednim punktem, ewentualny brak możliwości uniknięcia dekoherencji ani jej właściwego kompensowania, może być fundamentalną (podstawowej natury fizycznej) barierą dla implementacji skalowalnego, uniwersalnego komputera kwantowego, który stwarza ważne uzasadnienie dla kryptografii kwantowej (niemożliwość jednak stwierdzenia,

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

czy komputer kwantowy uda się zrealizować czy nie jest wystarczającym powodem dla prac w kierunku komercjalizacji kryptografii kwantowej, ponieważ w obliczu powstania komputera kwantowego wszystkie niejawne informacje szyfrowane klasycznie zostałaby natychmiast skompromitowane i ujawnione – dlatego w sytuacji braku pewności co do możliwości lub braku możliwości w sensie dopuszczalności prawami fizyki skonstruowania skalowalnego komputera kwantowego – kryptografia kwantowa powinna być już szeroko wdrażana)

8. Ocena krytyczna wyników prac badawczych projektu

W toku realizacji projektu „Prace badawczo-rozwojowe w kierunku komercjalizacji kryptografii kwantowej w układach bezsplątaniowych i splątaniowych" w ramach przeprowadzonych badań rozpoznano możliwości oraz uwarunkowania techniczne dla przygotowania do wdrożenia i komercjalizacji układów kryptografii kwantowej wykorzystującej protokoły zarówno nieoparte jak i oparte na splątaniu kwantowym. Uwarunkowania techniczne obecnego stanu rozwoju optyki kwantowej dla celów zastosowań w rzeczywistych sieciowych środowiskach komercyjnych były testowane w toku badań przemysłowych i prac rozwojowych w warunkach laboratoryjnych. Badania zakończyły się osiągnięciem z sukcesem celów projektowych i zakładanych wskaźników projektowych (w tym z ich przekroczeniem). W szczególności zrealizowane badania pozwoliły przeprowadzić pilotażowe wdrożenia obu rodzajów prototypowych układów QKD (bezsplątaniowych i splątaniowych) w metropolitalnej sieci światłowodowej we Wrocławiu. W toku realizacji projektu dokonano eksperymentalnego wdrożenia we Wrocławiu jednej z pierwszych na świecie prototypowych metropolitalnych sieci kwantowych QKD łączących splątaniową i bezsplątaniową komunikację kwantową (w czasie prowadzenia eksperymentalnych wdrożeń metropolitalnych w miejskiej infrastrukturze światłowodowej w latach 2013 i 2014 hybrydowe sieci QKD łączące układy splątaniowe i bezsplątaniowe były eksperymentalnie wdrażane poza Wrocławiem tylko w Wiedniu i w Tokio – co uczyniło z Wrocławia trzecie miasto na świecie, które dysponowało taką siecią w szkieletowej infrastrukturze telekomunikacyjnej).

Szczegółowe wyniki badań i prac rozwojowych w projekcie zostały upowszechnione w formie publikacji w międzynarodowych czasopismach specjalistycznych, oraz w formie prezentacji na międzynarodowych konferencjach w dziedzinie kryptografii kwantowej. W szczególności wyniki projektu prezentowano na następujących międzynarodowych konferencjach:

- 2nd Annual International Conference on Quantum Cryptography QCrypt 2012,
  10 – 14 wrzesień 2012, Singapur
- 3rd Annual International Conference on Quantum Cryptography QCrypt 2013,
  5 – 9 sierpień 2013, Waterloo, Kanada
- 1st Quantum Cryptography Standardization Symposium - Quantum-Safe-Crypto Workshop,
  26 – 27 wrzesień 2013, ETSI headquarters, Sophia Antipolis, Francja
- 5th LFPPI Symposium on Progress in Quantum Cryptography - seQre2014,
  27 - 28 styczeń 2014, Wrocław, Polska

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

- 4th International Conference on Advanced Communications and Computation - INFOCOMP 2014, 20 – 24 lipiec 2014, Paryż, Francja, gdzie prezentowanym wynikom badawczym przyznano I nagrodę za najlepszą pracę naukową przedstawioną na konferencji.

Ponadto, zgodnie z deklaracjami w projekcie, szczegółowe wyniki realizacji badań przemysłowych i prac rozwojowych zostały także zebrane i udostępnione na otwartej platformie internetowej http://www.seqre.net.

Część wyników projektu podlega obecnie procedurze zapewnienia ochrony własności intelektualnej w toku procedur patentowych przy wsparciu programu PatentPlus. Firma przygotowuje się równocześnie do kolejnego etapu wdrożeniowego polegającego na wprowadzeniu innowacyjnych, strategicznych i perspektywicznych produktów oraz usług opartych na wynikach badań przemysłowych i prac rozwojowych projektu do swojej oferty komercyjnej. W tym celu firma prowadzi działania w kierunku zapewnienia finansowania inwestycyjnego koniecznego do uruchomienia działań wdrożeniowych i produkcyjnych (prowadzone są rozmowy nt. inwestycji potrzebnych do wdrożenia linii produkcyjnych układów QKD z prywatnymi inwestorami i funduszami inwestycyjnymi typu Venture Capital oraz z instytucjami wsparcia inwestycyjnego, m.in. z Bankiem Gospodarstwa Krajowego, a także przygotowania do pozyskania funduszy inwestycyjnych w programie PO IR oraz w programie Bridge Venture Capital Narodowego Centrum Badań i Rozwoju). W dłuższej perspektywie komercjalizacja wyników badań projektowych zapewni wzrost przychodów i rentowności firmy w ramach wdrożeń komercyjnych planowanych w okresie trwałości projektu.

Poza wzrostem konkurencyjności oferty firmy realizatora projektu, istotnym rezultatem badań projektowych jest rozwój samej technologii kryptografii kwantowej, która ma duży potencjał dla unowocześnienia i zwiększenia konkurencyjności gospodarki krajowej względem gospodarek państw wysoko rozwiniętych, jak również strategiczne znaczenie dla bezpieczeństwa narodowego.

Osiągnięte w toku realizacji projektu wyniki prac badawczo-rozwojowych zostały przedstawione międzynarodowemu środowisku badawczemu w dziedzinie kryptografii kwantowej, a także komercyjno-rządowym sektorom potencjalnych odbiorców kryptografii kwantowej na specjalnie zorganizowanej w tym celu przez realizatora projektu międzynarodowej konferencji-sympozjum SEQRE 2014 (stanowiącej specjalną edycję w serii tradycyjnych sympozjów LFPPI na Politechnice Wrocławskiej) - http://www.seqre.net/seqre2014 - w dniach 27 i 28 stycznia 2014 roku.

Konferencja SEQRE 2014 prezentująca w międzynarodowym środowisku badawczym w tej dziedzinie wyniki realizacji projektu odbyła się pod honorowym patronatem Rektora Politechniki Wrocławskiej, Prezydenta Wrocławia oraz Dyrektora Narodowego Centrum Badań i Rozwoju. Skupiła ona najwybitniejszych światowych naukowców w dziedzinie kryptografii kwantowej, w tym twórców tej dziedziny, zaproszonych przez realizatora projektu i zespół naukowy odpowiedzialny za realizację badań. Poza prezentacją wyników badań zrealizowanych w projekcie, wykłady plenarne dotyczące światowych osiągnięć naukowych i technicznych w dziedzinie kryptografii kwantowej wygłosili m.in. prof. N. Gisin (Genewa), prof. A. Ekert (Oxford, Singapur), a także czołowi światowi technolodzy w tej dziedzinie: prof. V. Makarov (Waterloo), dr. A. Poppe (Wiedeń), dr. K. Tamaki (Tokio), dr. M. Lucamarini (Cambridge), dr. S. Kunz-Jacques (Paryż). Związane z problematyką kryptografii kwantowej krajowe teoretyczne badania podstawowe przedstawili prof. J. Rembieliński (Łódź) oraz prof. M. Czachor (Gdańsk). Przedstawiciele zespołu projektowego angażowanego przez realizatora projektu przedstawili szczegółowe wyniki badań przemysłowych i prac rozwojowych osiągniętych w

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

projekcie do czasu organizacji konferencji oraz przeprowadzili szeroko zakrojone demonstracje technologiczne i specjalistyczne szkolenia w zakresie splątaniowej i bezsplątaniowej kryptografii kwantowej. O szczegółach innych światowych wdrożeń opowiedzieli przedstawiciele najważniejszych firm komercjalizujących kryptografię kwantową w innych krajach, w szczególności w Austrii, Szwajcarii, Francji, Wielkiej Brytanii oraz Japonii przedstawiając także demonstracje technologiczne.

W konferencji udział wzięli wysokiej rangi wojskowi przedstawiciele Ministerstwa Obrony Narodowej w ramach utworzonej w 2013r. struktury MON - Narodowego Centrum Kryptologii oceniający postęp w badaniach realizowanych w projekcie pod względem potencjału dla strategicznego bezpieczeństwa narodowego. Przedstawiciele MON/NCK zadeklarowali wysokie zainteresowanie technologią jako perspektywiczną dla bezpieczeństwa narodowego, niemającą klasycznych odpowiedników dla zapewnienia teoretycznie bezwarunkowego bezpieczeństwa tajnej komunikacji w zastosowaniach wojskowych. Reprezentowane były także banki zainteresowane komercyjnymi wdrożeniami tej technologii. Potencjalnym odbiorcom komercyjnym, również deklarującym zainteresowanie przyszłymi wdrożeniami przedstawiono szczegóły uzyskanych wyników projektowych w kontekście uwarunkowań wdrożeń w rzeczywistych środowiskach komercyjnych sieci metropolitalnych.

Wyniki badań oraz demonstracje technologiczne osiągnięte w projekcie zostały uznane przez komisję powołaną przez Prezydenta Wrocławia za jeden z „7 cudów Wrocławia", który zgodnie z deklaracją organizatorów będzie prezentowany w kategorii Nauka w ramach specjalnej wystawy z okazji obchodów dni Wrocławia jako Europejskiej Stolicy Kultury w 2016 roku.

Realizowane badania przemysłowe miały wysoce zaawansowany charakter ulokowany w obszarze inżynierii i optyki kwantowej. Ich realizacja była możliwa przy zaangażowaniu dobrze przygotowanych kadr merytorycznych firmy oraz ścisłej współpracy z wiodącymi w tej dziedzinie ośrodkami naukowymi (w tym krajowymi i zagranicznymi). W projekcie zapewniono udział kadr naukowych (w tym zespołów naukowych Laboratorium Kryptografii Kwantowej przy Katedrze Technologii Kwantowych Politechniki Wrocławskiej – nowego laboratorium stworzonego w ramach ogólnokrajowego projektu Narodowego Laboratorium Technologii Kwantowych NLTK oraz wrocławskiego oddziału krajowej sieci naukowej KBN Laboratorium Fizycznych Podstaw Przetwarzania Informacji LFPPI, jak również Katedry Bezpieczeństwa Systemów Informatycznych na Politechnice Wrocławskiej) w formie współpracy polegającej na zleceniu realizacji części prac badawczych i ogólnej współpracy badawczej. Udział kadr naukowych Katedry Bezpieczeństwa Systemów Informatycznych PWr. był dla tego typu badań istotnym osiągnięciem międzynarodowym polegającym na zapewniu interdyscyplinarnego charakteru badań nad kryptografią kwantową zarówno z perspektywy fizyki/mechaniki kwantowej oraz informatyki/teorii komunikacji – wyraz temu dała I nagroda za najlepszą pracę naukową na światowej konferencji the 4th International Conference on Advanced Communications and Computation - INFOCOMP 2014, realizowanej 20 – 24 lipca 2014 w Paryżu. Do zadań badawczych angażowani byli specjaliści o wykształceniu z zakresu informatyki i fizyki i odpowiednich umiejętnościach i doświadczeniu (zgodnie z założeniami projektowymi zapewniony był też udział studentów studiów inżynierskich/magisterskich i doktorantów fizyki/informatyki PWr realizujących prace dyplomowe z zakresu kryptografii kwantowej w zespole LKK NLTK PWr). W toku realizacji projektu zaawansowano jeden przewód doktorski oraz 2 prac magisterskie w bezpośrednim powiązaniu z zaplanowanymi pracami badawczymi. W projektach obecna była również współpraca z międzynarodowymi ekspertami zagranicznymi i członkami zespołów badawczych wiodących ośrodków badań nad kryptografią kwantową na świecie, m.in.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

IdQuantique SA i Uniwersytet w Genewie oraz Austrian Institute of Technology AIT i Uniwersytet w Wiedniu. Zrealizowane w projekcie badania przemysłowe i prace rozwojowe miały także komplementarny charakter względem badań podstawowych w obszarze informatyki i inżynierii kwantowej prowadzonych równolegle na świeci (w tym przez partnerów zagranicznych) oraz w kraju na Politechnice Wrocławskiej (Instytut Fizyki) i w ośrodkach krajowej sieci naukowej KBN Laboratorium Fizycznych Podstaw Przetwarzania Informacji (grupującej około 20 polskich instytucji naukowych prowadzących badania w zakresie informatyki kwantowej przy udziale m.in. Uniwersytetu Warszawskiego, Uniwersytetu Jagiellońskiego, Politechniki Wrocławskiej, Centrum Fizyki Teoretycznej PAN w Warszawie, Instytutu Fizyki PAN w Warszawie, Uniwersytetu Gdańskiego, UMK w Toruniu, Uniwersytetu Łódzkiego, UMCS w Lublinie, AGH w Krakowie, UMK w Poznaniu i będącej realizatorem projektu zamawianego MNiI pt. „Informatyka kwantowa i inżynieria kwantowa" oraz współrealizatorem wielu innych projektów w skali krajowej i międzynarodowej) jak również Narodowego Laboratorium Kryptografii Kwantowej (konsorcjum założonego z inicjatywy Narodowego Centrum Badań i Rozwoju oraz sieci LFPPI, realizującego obecnie ogólnokrajowy projekt aparaturowy w zakresie technologii kwantowych o łącznym budżecie 75 mln zł). Koordynatorem projektu był prof. dr hab. inż. L. Jacak kierownik Zespołu Teorii Fazy Skondensowanej Instytutu Fizyki PWr, kierownik NLTK (w tym LKK, Laboratorium Kryptografii Kwantowej) oraz kierownik LFPPI przy PWr (były dyrektor Instytutu fizyki oraz były prorektor PWr.). Zespół naukowy z Instytutu Fizyki Politechniki Wrocławskiej pod kierunkiem prof. Jacaka, prowadził badania w zakresie informatyki kwantowej od wielu lat (w tym w zakresie kryptografii kwantowej i dekoherencji – głównej przeszkody w rozwoju technologii kwantowych). Dużą część zespołu badawczego stanowią młodsi pracownicy naukowi, a także doktoranci i magistranci (młodsi przedstawiciele zespołu badawczego wnioskodawcy uczestniczyli m.in. w zorganizowanej przez idQuantique SA i Uniwersytet Genewski „I Międzynarodowej Zimowej Szkole Praktycznej Kryptografii Kwantowej" w LesDiablerets w Szwajcarii w styczniu 2009r., gdzie brali udział w badaniach prowadzonych w ramach eksperymentalnych i komercyjnych układów dystrybucji klucza kwantowego w modelu bezsplątaniowym).

W toku realizacji projektu w firmie zostało utworzone i odp. wyposażone Centrum Badań i Rozwoju, stanowiące komórkę realizacji badań przemysłowych i prac rozwojowych w kierunku ich wdrożeń rynkowych. Zakres działalności Centrum Badawczo-Rozwojowego firmy, został określony w następującym zakresie:

- Głównym celem Centrum B+R jest prowadzenie prac badawczo-rozwojowych zmierzających do wytwarzania i wdrażania nowych technologii w dziedzinach działalności firmy, a w obszarze współpracy z nowoutworzonym Centrum Kryptografii Kwantowej badania i rozwój w zakresie tej technologii
- Drugorzędnym celem Centrum B+R jest zapewnienie odpowiedniej ochrony własności intelektualnej i przemysłowej, wykonywanie badań i analiz oraz ekspertyz technicznych w dziedzinach prowadzonych badań, jak również prowadzenie prac rozwojowych w zakresie już wytworzonych lub wdrożonych technologii (w szczególności planuje się współpracę Centrum B+R z Centrum Kryptografii Kwantowej, w kierunku bieżącego rozwoju wdrażanych technologii)
- Trzeciorzędnym celem Centrum B+R jest inicjowanie i nadzorowanie współpracy badawczo-rozwojowej z zewnętrznymi podmiotami, jak również upowszechnianie wyników prac badawczo-rozwojowych (m.in. w formie publikacji, organizacji konferencji i sympozjów, przedstawiania prezentacji konferencyjnych, etc.), w szczególności w obszarze współpracy z

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

CKK planuje się poszerzenie współpracy B+R z wiodącymi na świecie firmami i ośrodkami badawczymi komercjalizującymi kryptografię kwantową.

Struktura organizacyjna i zarządzanie Centrum B+R:

1. Centrum B+R jest działem wewnętrznym (wewnętrzną komórką organizacyjną) spółki CompSecur sp. z o.o. i podlega jej Zarządowi, który określa zasady jej funkcjonowania i strukturę organizacyjną Centrum B+R
2. Pracami Centrum B+R kieruje Dyrektor Centrum B+R
3. Ciałem pełniącym merytoryczną funkcję doradczą i opiniującą jest Rada Naukowa Centrum B+R
4. Dyrektor Centrum B+R powoływany jest przez Zarząd na określony lub nieokreślony czas pełnienia swojej funkcji i podlega bezpośrednio Zarządowi spółki, któremu składa bieżące raporty z działalności badawczo-rozwojowej
5. Członkowie Rady Naukowej Centrum B+R zapraszani są do członkostwa przez Zarząd na określony lub nieokreślony czas jego trwania (w skład Rady Naukowej mogą wchodzić zaproszeni eksperci zewnętrzni lub pracownicy spółki)
6. Dyrektor Centrum B+R w konsultacji z Radą Naukową określa strategiczne roczne plany ramowe działalności Centrum B+R i nadzoruje ich prawidłowy przebieg
7. Dyrektorowi Centrum B+R w zakresie merytorycznej działalności podlegają specjaliści zatrudniani przez spółkę CompSecur sp. z o.o. w obszarze ich zaangażowania w działalność badawczo-rozwojową
8. Działalność Centrum B+R w zakresie realizacji jego celów prowadzona jest w toku wyodrębnionych organizacyjnie projektów B+R, a w przypadku mniej złożonych prac w toku bieżącej aktywności Centrum
9. Centrum B+R działa zgodnie z założeniami Polityki bezpieczeństwa obowiązującej w spółce, w szczególności odpowiednio chroniąc wyniki prac badawczo-rozwojowych
10. Prace Centrum B+R są przedmiotem audytu i certyfikacji wdrożonego w spółce systemu zarządzania jakością wg normy ISO 9001:2008.

Obszary merytorycznej działalności Centrum B+R:

1. Bezpieczeństwo informatyczne
    a. Kryptografia kwantowa
    b. Kryptografia klasyczna
    c. Sprzętowe zabezpieczenia informatyczne
    d. Programowe zabezpieczenia informatyczne
    e. Inne technologie zabezpieczeń informatycznych

2. Informatyka i komunikacja kwantowa
    a. Algorytmy kwantowe
    b. Układy przetwarzające informację kwantową
    c. Komputery kwantowe
    d. Teleportacja kwantowa
    e. Sieci kwantowe

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

3. Klasyczne technologie informatyczne i komunikacyjne
    a. Platformy zdalnej komunikacji
    b. Technologie e-learningowe
    c. Technologie telepracy
    d. Systemy sieciowe
    e. Aplikacje mobilne
4. Inne zaawansowane technologie

9. Wnioski płynące z realizacji I Etapu projektu

Badania przemysłowe i prace rozwojowe realizowane w ramach I Etapu projektu zakończyły się sukcesem, tj. pełnym osiągnięciem celów projektu, w tym przygotowaniem na poziomie know-how oraz technologii do produkcji komercyjnych układów kryptografii kwantowej bezsplątaniowej i splątaniowej oraz do ich wdrożenia rynkowego na rynku krajowym i międzynarodowym.

Osiągnięte rezultaty badawczo-rozwojowe (w tym wdrożona prototypowa metropolitalna sieć kwantowa QKD integrująca kwantową komunikację splątaniową i bezsplątaniowej we Wrocławiu, zaledwie trzecia na świecie po Tokio i Wiedniu) wymagają obecnie inwestycji infrastrukturalnych i technologicznych (linia produkcyjna) w celu wprowadzenia produktów komercyjnych na rynek (wraz z towarzyszącymi działaniami marketingowymi) i rozpoczęcia właściwej sprzedaży (głównie w sektorach finansowym oraz administracji publicznej, jak również wojskowym). Wynikami realizowanych prac B+R są prawa własności intelektualnej (w tym prawa do „know-how", autorskie prawa majątkowe do utworów, prawa do uzyskania patentów oraz obecnie w przygotowaniu patenty, wzory przemysłowe i użytkowe o międzynarodowym zasięgu ochrony prawnej) w zakresie prototypowych systemów QKD, dokumentacji technicznych i ekspertyz oraz opracowań badawczych, w tym w szczególności: prototypowe wersje systemów QKD, oparte na podsystemach zewnętrznych producentów – umożliwiające produkcję komercyjną układów QKD na bazie dostępnych komercyjnie komponentów składowych układów optycznych i interfejsów sterowania opto-elektronicznego, zarówno w reżimie splątaniowym i bezsplątaniowym; szereg publikacji badawczych oraz ekspertyz technicznych nt. prototypowych systemów QKD, ich architektur, komponentów, parametrów, koncepcji protokołowych; dokumentacje techniczna koncepcji prototypowych i systemów QKD; pierwsza w kraju i jedna z pierwszych na świecie metropolitalna sieć kwantowa (QKD) we Wrocławiu; zgłoszenia wzorów przemysłowych i użytkowych oraz wnioski patentowe (w przygotowaniu przy wsparciu zasięgu międzynarodowego ochrony własności intelektualnej w programie PatentPlus).

Podczas gdy komputery kwantowe stają się rzeczywistością (już w maju 2013 roku NASA i Google we wspólnym przedsięwzięciu wdrożyły 512 qubitowe nadprzewodzące komputery kwantowe DWave Two, tworząc pierwsze na świecie kwantowe laboratorium sztucznej inteligencji, a od tego czasu nastąpił cały szereg przełomowych rezultatów na drodze do budowy uniwersalnego komputera kwantowego – więcej informacji w sekcji Aktualności na platformie internetowej projektu http://seqre.net/news) bezpieczeństwo krytycznej, tajnej komunikacji podlega procesowi przewartościowania. Klasyczne kryptosystemy, opierające się na matematycznych problemach trudnych zostały zakwestionowane, jako że problemy te mogą być skutecznie rozwiązane przez komputery kwantowe, w badaniach nad którymi obecnie osiąganych jest coraz więcej przełomów

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

technologicznych. Z nadchodzącą rewolucją informatyki kwantowej wiąże się coraz szerzej dostrzegane zagrożenie dla rozmaitych zabezpieczeń komunikacji o kluczowej roli dla instytucji sektora finansów i bankowości, a także w wymiarze pozakomercyjnym o charakterze bezpieczeństwa narodowego dla administracji publicznej i wojska. W tym kontekście przygotowanie technologiczne dla wdrożenia rynkowego krajowych systemów kryptografii kwantowej jest bardzo istotne i posiada poza komercyjnym również aspekt strategiczny, związany z bezpieczeństwem narodowym.

Kryptografia kwantowa stanowi jedyne pewne zabezpieczenie tajnej komunikacji zdalnej przed ewentualnym atakiem na szyfry z wykorzystaniem komputera kwantowego nad konstrukcją którego trwają zaawansowane już prace, oferując równocześnie po raz pierwszy w historii teoretycznie bezwarunkowy poziom bezpieczeństwa komunikacji, możliwy do wdrożenia w obecnie stosowanych infrastrukturach telekomunikacyjnych, co udowodniono w toku pilotażowych wdrożeń prototypów w metropolitalnej sieci wrocławskiej (warto podkreślić, że w czasie prowadzenia eksperymentalnych wdrożeń metropolitalnych w miejskiej infrastrukturze światłowodowej hybrydowe sieci QKD łączące układy splątaniowe i bezsplątaniowe były eksperymentalnie wdrażane poza Wrocławiem tylko w Wiedniu i w Tokio – co uczyniło z Wrocławia trzecie miasto na świecie, które dysponowało taką siecią w szkieletowej infrastrukturze telekomunikacyjnej).

Wyniki badawcze projekty dotyczą technologii o charakterze strategicznym dla bezpieczeństwa narodowego kraju oraz o perspektywicznym potencjale rynkowym w sektorze finansowym, administracyjnym i wojskowym. Na poziomie teoretycznym, po raz pierwszy w historii kryptografii, QKD pozwala na uzyskanie bezwarunkowego bezpieczeństwa komunikacji dzięki fundamentalnym prawom fizyki (mechaniki kwantowej). Obecnie upowszechnione, tzw. asymetryczne systemy kryptograficzne (stosowane w szyfrach i podpisach cyfrowych w Internecie) oferują jedynie warunkowe (obliczeniowe) bezpieczeństwo komunikacji, które w wymiarze jakościowym zostanie całkowicie zniesione po zbudowaniu skalowalnego komputera kwantowego (obecnie dostępna II generacja nadprzewodzącego tzw. adiabatycznego i nieuniwersalnego procesora komputera kwantowego DWave Two ma 512 qubitów i stanowi ważny przełom technologiczny co potwierdza zakup licznych systemów przez Google i NASA oraz Lockheed Martin za dziesiątki mln USD świadczący o rzeczywistym potencjale tej technologii). Druga generacji nadprzewodzących komputerów kwantowych działających w reżimie tzw. adiabatycznego przetwarzania informacji kwantowej pozwala na realizację szerokiej względem zastosowań klasy algorytmów kwantowego wyżarzania, bardzo istotnych w szczególności w dziedzinie kluczowych problemów optymalizacyjnych i heurystycznych, sztucznej inteligencji, rozpoznawania obrazów i wreszcie kryptograficznych szyfrów asymetrycznych. Rozwój informatycznych technologii kwantowych, określanych jako technologie przełomowe, lub disruptive technologies w ocenie ekspertów m.in. z Joint-Research Center Komisji Europejskiej zainicjują kolejną intensywną rewolucję informacyjno-komunikacyjną. Jej ważnym aspektem będzie fakt, że dotychczas stosowane szyfry i podpisy cyfrowe oparte na kryptografii klasycznej będą narażone na natychmiastowe złamanie, a cała zabezpieczona nimi poufna i wiarygodna komunikacja (także archiwalna) ujawniona oraz podatna na utratę wiarygodności (w następstwie złamania podpisów cyfrowych). Technologiczna implementacja systemów kryptografii kwantowej, jedynego zabezpieczenia przed komputerami kwantowymi, odbywa się w reżimie optyki kwantowej i wymaga bardzo precyzyjnych komponentów obejmujących odp. tłumione lasery, interferometry i polaryzatory, detektory pojedynczych fotonów oraz światłowody, jak również koncepcje architektur układów oraz implementacje sterujących systemów elektronicznych i oprogramowania.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

Wyniki badawcze projektu w znaczący sposób zwiększyły intensywność działań w zakresie komercjalizacji technologii kryptografii kwantowej w Unii Europejskiej i są unikalne w skali kraju. Wnioskodawca jako akademicka spółka spin-off zajmującej wysokie pozycje w niezależnych rankingach uczelni wyższej, współtworzona przez kilkunastu pracowników naukowych będących międzynarodowymi ekspertami w zakresie bezpieczeństwa IT oraz w dziedzinie informatyki i kryptografii kwantowej, ma dzięki swoim dotychczasowym ponad 10-letnim udanym doświadczeniom rynkowym duże szanse na powodzenie w realizacji prac wdrożeniowych i komercjalizacyjnych w kraju i za granicą, które planuje jako naturalny, kolejny etap po zrealizowanych zaawansowanych badaniach przemysłowych i pracach rozwojowych w obszarze prototypowych systemów kryptografii kwantowej (zakończonych prototypowymi wdrożeniami w sieci metropolitalnej miasta). Jako spółka realizująca jedyne w kraju projekty badań przemysłowych ukierunkowanych na wdrożenie kryptografii kwantowej, a także spin-off mający w ramach współpracy z siecią naukową KBN Laboratorium Fizycznych Podstaw Przetwarzania Informacji LFPPI oraz Narodowym Laboratorium Technologii Kwantowych NLTK (NLTK zostało założone z inicjatywy Narodowego Centrum Badań i Rozwoju oraz LFPPI - jest realizatorem dużego projektu aparaturowego w zakresie technologii kwantowych o łącznym budżecie 75 mln zł, w tym na PWr 8 mln zł) dostęp do unikalnych w skali krajowej ale także w skali ogólnoświatowej fizycznych laboratoriów kwantowych, a także dzięki współpracy badawczej kadr naukowych współtworzących spółkę i uczestniczących w organizacji sieci naukowej LFPPI i laboratorium NLTK przy Katedrze Technologii Kwantowych PWr z międzynarodowymi ekspertami w dziedzinach inżynierii, informatyki i kryptografii kwantowej, wnioskodawca jest jedną z niewielu firm w krajowym sektorze high-tech o potencjale umożliwiającym udaną komercjalizację kryptografii kwantowej w Polsce.

Wyrazem powyższej sytuacji było zorganizowane przez spółkę i jej partnerów akademickich (LFPPI/NLTK/PWr), odbywające się w styczniu 2014 roku V Sympozjum LFPPI - Progress in Quantum Cryptography - seQre2014, które stanowiło unikalne w skali międzynarodowej spotkanie ekspertów i firm wdrażających kryptografię kwantową z przedstawicielami sektorów IT/ICT, finansów i bankowości oraz administracji publicznej i wojska, jak również innych instytucji zainteresowanych potencjalnymi wdrożeniami tej nowej technologii, mając za zadanie przedstawienie aktualnego stanu rozwoju praktycznych implementacji i wdrożeń kryptografii kwantowej, które pomimo dużego stopnia innowacyjności technicznej w obszarze technologii kwantowej, na świecie realizowane są już na coraz szerszą skalę - m.in. wdrożenia w sektorze bankowości, szczególnie w Szwajcarii oraz Luksemburgu, a także w Japonii, USA, Austrii, czy w Niemczech. Sympozjum seQre2014 (http://seqre.net/seqre2014) skupiło najwybitniejszych specjalistów w zakresie kryptografii kwantowej w tym jej autorów i twórców. Wykłady plenarne wygłosili m.in. prof. N. Gisin (pionier komercjalizacji kryptografii kwantowej na świecie oraz założyciel pierwszej firmy specjalizującej się w kryptografii kwantowej – genewskiej IDQuantique SA), prof. A. Ekert (pochodzący z Wrocławia autor koncepcji splątaniowej kryptografii kwantowej z 1992r., kierownik katedry na Uniwersytecie w Oxfordzie i Dyrektor Centrum Technologii Kwantowych w Singapurze), prof. V. Makarov (Dyrektor Laboratorium Kryptografii Kwantowej przy Instytucie Informatyki Kwantowej Uniwersytetu w Waterloo oraz główny konsultant technologiczny firm aktywnie komercjalizujących kryptografię kwantową), dr A. Poppe (główny ekspert techniczny kryptografii kwantowej AIT - Austrian Institute of Technology światowego pioniera i obecnego lidera splątaniowej kryptografii kwantowej z Wiednia), dr K. Tamaki (główny inżynier projektu kwantowej sieci w Tokio, realizowanej przez konsorcjum japońskiej narodowej firmy telekomunikacyjnej NTT oraz szeregu japońskich instytucji badawczych),

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

prof. M. Kuś (Przewodniczący Rady Naukowej Krajowego Centrum Informatyki Kwantowej w Gdańsku), jak również przedstawiciele wszystkich firm na świecie, które aktywnie komercjalizują kryptografię kwantową: IDQuantique SA (Genewa), AIT (Wiedeń), SeQureNet SA (Paryż), MagiQ Inc. (Nowy Jork), Toshiba (Cambridge/Tokio), NTT (Tokio) wraz z towarzyszącymi demonstracjami technologicznymi. Sympozjum, odbywające się pod patronatem honorowym Rektora Politechniki Wrocławskiej, Prezydenta Wrocławia i Dyrektora Narodowego Centrum Badań i zakończyło się znaczącym sukcesem pozwalając na zainicjowanie i poszerzenie współpracy badawczej z wiodącymi na świecie ośrodkami w tej dziedzinie (m.in. CQT w Singapurze, NTT w Tokio, Sandia Laboratories - Lockheed Martin w Albuquerque, AIT w Wiedniu, LTCI / CNRS – Telecom ParisTech w Paryżu, Toshiba R&D Center w Cambridge, IDQuantique w Genewie oraz licznymi zagranicznymi Uniwersystetami - jak również podmiotami krajowymi -- Narodowe Centrum Kryptologii w ramach MON, Biuro Bezpieczeństwa Narodowego, laboratorium FAMO w Toruniu, centrum KCIK w Gdańsku i inne). Sympozjum zostało zorganizowane z okazji zakończenia prac badawczo-rozwojowych prowadzonych w kraju projektów w obszarze kryptografii kwantowej przez CompSecur/LFPPI/NLTK/PWr i przedstawienia ich rezultatów w formie demonstracji technologicznych oraz prototypowej metropolitalnej sieci kwantowej we Wrocławiu (http://seqre.net/seqre2014/wroclaw.php), zaznaczających silną pozycję kraju na technologicznej mapie świata (sieć metropolitalna QKD, funkcjonująca w strukturze szkieletowej miejskiej sieci światłowodowej we Wrocławiu i jest trzecią na świecie siecią po Tokijskiej i Wiedeńskiej, która integruje prototypowe systemy splątaniowe i bezsplątaniowe QKD – można powiedzieć, że rewolucjonizują one tradycyjną telekomunikację w zakresie bezpieczeństwa wymiany danych – według ogólnej oceny środowisk akademickich fizyków, informatyków i elektroników technologie informatyki kwantowej i komunikacji kwantowej stanowią przeskok technologiczny innego rodzaju niż ewolucja telegrafu w kierunku komunikacji cyfrowej, ponieważ dotyczą zmiany reżimu komunikacji z praw fizyki klasycznej na prawa mechaniki kwantowej). Światowy poziom rezultatów prowadzonych przez wnioskodawcę prac B+R w zakresie przygotowań do komercjalizacji kryptografii kwantowej został przedstawiony na forum międzynarodowej społeczności ekspertów kryptografii kwantowej w trakcie współorganizowanego przez Wnioskodawcę w dniach 27-28 stycznia 2014 roku Sympozjum seQre2014 – Postęp w kryptografii kwantowej, połączony z dynamicznym rozwojem eksportu przez firmę specjalistycznych usług szkoleniowo-konsultingowych w zakresie bezpieczeństwa informatycznego na rynkach europejskich, a także na rynku japońskim (zgodnie z wdrażaną strategią opracowaną przy współpracy z Polsko-Japońską Izbą Gospodarczą i Japan External Trade Organization JETRO) pozwala oczekiwać, że sukces w zakresie komercjalizacji kryptografii kwantowej w kraju może być jednym z czynników korzystnie wpływających na bilans handlowy z rozwiniętymi gospodarkami w kategoriach poziomu zaawansowania technologicznego (wspierając wysiłki na rzecz unowocześniania krajowej gospodarki i tworzenia ją bardziej konkurencyjną względem gospodarek państw wysoko rozwiniętych, również w zakresie bilansu handlowego Polski w obszarze zaawansowanych technologii high-tech).

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.

10. Szczegółowe wyniki prac badawczych

Wszystkie opracowania merytoryczne (w tym sprawozdania dot. wyników badań oraz publikacje zawierające szczegółowe jawne wyniki prac badawczych) znajdują się na stronach platformy komercjalizacji kryptografii kwantowej – http://seqre.net.

Niniejszy dokument jest poufny i stanowi tajemnicę gospodarczą przedsiębiorstwa CompSecur sp. z o.o. Może być przetwarzany tylko przez prawnie dopuszczone do tego podmioty w związku z realizacją projektu "Wsparcie procedur patentowych i ochrony prawwłasności przemysłowej w obszarze komercjalizacji kryptografii kwantowej" (nr umowy PP3/W-32/D-2223/2014 w ramach wsparcia finansowego Narodowego Centrum Badań i Rozwoju) w granicach uregulowanych prawem.