Olbrzymi postęp dokonany w dziedzinie eksperymentalnej optyki kwantowej na przestrzeni ostatnich dekad, pozwalający na efektywną kontrolę oraz inżynierię kwantowych stanów światła i materii, zapoczątkował tzw. drugą rewolucję kwantową. Rozmaite technologie kwantowe są obecnie intensywnie rozwijane, aby umożliwić ich pełnowymiarowe zastosowanie praktyczne. Wszystkie one oparte są na wykorzystaniu zjawiska kwantowego splątania, zdolnego do wytworzenia idealnych korelacji pomiędzy różnymi układami kwantowymi, będącymi z natury obiektami probabilistycznymi. Z tego względu dystrybucja splątania pomiędzy odległymi użytkownikami jest niezwykle istotnym zadaniem, zarówno w kontekście technologii kwantowych, jak i badania podstawowych praw przyrody. Z drugiej strony rozwój komputerów kwantowych stanowi potencjalne zagrożenie bezpieczeństwa całej poufnej komunikacji prowadzonej za pomocą kryptografii klasycznej. Jest tak, ponieważ poprzez użycie algorytmów kwantowych są one w stanie rozwiązywać skomplikowane problemy obliczeniowe, leżące u podstaw powszechnie stosowanych metod kodowania klasycznego. Tymczasem protokoły kwantowej dystrybucji klucza kryptograficznego (QKD – od ang. *quantum key distribution*) bazują na detekcji splątania kwantowego, bezpośrednio lub pośrednio rozdzielonego pomiędzy upoważnionych użytkowników. Dzięki temu, bezpieczeństwo komunikacji kwantowej opiera się nie na domniemanej trudności przeprowadzenia obliczeń matematycznych, lecz na fundamentalnych prawach natury i może zostać zweryfikowane za pomocą dowodów teoretycznych.

Chociaż protokoły QKD były wielokrotnie testowane w praktyce, zarówno w laboratorium jak i poza nim, ich realizacje były zwykle przeprowadzane przy użyciu dedykowanych połączeń optycznych. Niemniej jednak, pełnowymiarowe zastosowanie bezpiecznej komunikacji kwantowej będzie wymagało realizacji tych schematów, jak również dystrybucji splątania, w środowisku istniejących sieci komunikacyjnych, gdzie kanały optyczne wykorzystywane są jednocześnie do transmisji danych przy pomocy multipleksowanych sygnałów klasycznych. Konieczne będzie również zwiększenie szybkości bezpiecznej komunikacji kwantowej, które może zostać osiągnięte poprzez multipleksowanie sygnałów kwantowych. Niestety, jednoczesna transmisja klasycznych i kwantowych danych w tym samym światłowodzie generuje zjawisko przesłuchu, skutkujące wzrostem szumu. Ponieważ moc sygnałów kwantowych jest o wiele rzędów wielkości mniejsza, niż w przypadku sygnałów klasycznych, szum ten ma niszczycielski wpływ na komunikację kwantową. Pomimo tego, badania prowadzące do realizacji multipleksowanej komunikacji kwantowej w koegzystencji z sygnałami klasycznymi były dotychczas prowadzone jedynie sporadycznie i tylko w przypadku wybranych protokołów.

W ramach proponowanego projektu planujemy wykonanie kompleksowej analizy powyższych zagadnień, celem opracowania stabilnych i efektywnych metod implementacji protokołów komunikacji kwantowej przy użyciu multipleksowanych sieci optycznych. Kolaboracyjny charakter projektu umożliwi przeprowadzenie tych badań w oparciu o dwa istotnie różne podejścia do komunikacji kwantowej, oparte na tzw. zmiennych dyskretnych oraz ciągłych, wykorzystujących odpowiednio korpuskularne oraz falowe właściwości światła kwantowego. Poprzez zbadanie zalet i wad każdego z tych podejść w obecności praktycznych niedoskonałości sprzętowych mamy zamiar opracować wzorce i najkorzystniejsze rozwiązania dla schematów dystrybucji splątania oraz QKD we wspomnianym środowisku. Przeanalizujemy również skalowalność błędów wynikających z niedoskonałości sprzętowych wraz ze wzrostem liczby węzłów sieci. Zaproponujemy rozwiązania, mające na celu kompensację tego efektu oraz zjawiska przesłuchu w oparciu o metody weryfikacji splątania oraz analizy bezpieczeństwa, modyfikację źródła splątania i układu eksperymentalnego lub też użycie metod przetwarzania danych. Otrzymane wyniki zostaną przedstawione grupom eksperymentalnym w celu ich weryfikacji oraz przeprowadzenia dalszych testów. Dzięki temu proponowany projekt przyczyni się do rozwoju zarówno teoretycznych badań fundamentalnych własności splątania kwantowego w przypadku wielomodowym, jak również praktycznej komunikacji kwantowej w niezwykle istotnym środowisku multipleksowanych sieci telekomunikacyjnych.