Jak wskazują badania, technologie informacyjne stanowią o niepomijalnym procencie zużycia zasobów energii na Ziemi. W ostatnich latach wzrosła także świadomość, że należy korzystać z jej zasobów w sposób przyjazny dla środowiska. Równolegle, do grona technologii informacyjnych dołączyła kwantowa informatyka – dziedzina wykorzystująca prawa fizyki, konkretnie mechaniki kwantowej w celu przetwarzania informacji. Kwantowa Informatyka, osiągnęła w ciągu ostatnich dekad wysoki stopień zaawansowania. Wraz z jej rozwojem odkryto i zbadano wiele tak zwanych zasobów kwantowych. Przez kwantowy zasób rozumiemy zjawisko, dzięki któremu w pewnych okolicznościach otrzymujemy szybsze, bardziej wydajne lub bardziej bezpieczne przetwarzanie informacji. Do listy znanych zasobów należą między innymi kwantowe splątanie, kwantowa koherencja, nielokalność typu Bella, kwantowa kontekstualność, bezpieczna losowość oraz klucz kryptograficzny bezpieczny względem kwantowego adwersarza, jednak jest ona ciągle wydłużana. Jak dotąd, badano zwykle jak otrzymać określony zasób, akceptując jednocześnie dowolnie duży koszt jego wytworzenia. W minionym roku powstała jednak kwantowa inicjatywa dla energii (Quantum Energy Initiative), której celem jest estymacja i minimalizacja zużycia zasobów fizycznych przez kwantowe technologie.

W myśl tej inicjatywy, pierwszym celem niniejszego projektu jest zaprojektowanie nowych protokołów otrzymywania zasobów kwantowych, które są bardziej przyjazne dla środowiska. Tym razem nie będzie jedynym celem uzyskanie zasobów, ale także minimalizacja kosztu energetycznego ich uzyskania. Jednym z wielu zasobów które będziemy badać jest tzw. „magiczność" która pozwala na uniwersalne kwantowe obliczenia, jak również kwantowa koherencja i czystość rozumiana jako możliwość wykonania pracy termodynamicznej.

Jednym z najważniejszych pod względem zastosowania zasobów kwantowych obok powyższych zasobów i kwantowego splatania jest także klucz kryptograficzny bezpieczny względem kwantowego adwersarza. W zależności od poziomu troski o bezpieczeństwo, to znaczy od zaufania do producenta urządzenia kryptograficznego generującego klucz kryptograficzny mówimy o kluczu którego bezpieczeństwo zależy bądź nie zależy od urządzenia. Co interesujące, teoria klucza kryptograficznego nie została rozwinięta w pełni do dnia dzisiejszego. Drugim celem niniejszego projektu jest rozwinięcie teorii klucza kryptograficznego. Po pierwsze przez obliczenie kosztu bezpieczeństwa dla dwuukładowych stanów kwantowych. Po drugie zamierzamy znaleźć ograniczenia górne na wieloukładowy koszt splątania kwantowego jak i bezpiecznego klucza. Najważniejszym czynnikiem wskazującym na wyciek energii w procesie przetwarzania informacji kwantowej jest nieodwracalność w procesie tworzenia zasobu i jego destylacji – otrzymywania zasobu z jego zaszumionej wersji. Zatem po trzecie chcemy określić wielkość takiej nieodwracalności, co pozwoli oszacowanie kosztu energetycznego w zależności od kosztu technologicznego przygotowania kubitów (jednostek kwantowej informacji) w odpowiednim stanie. W tym celu podamy nowe, ciasne ograniczenia górne na destylowalny klucz kryptograficzny w różnych scenariuszach oraz ograniczenia dolne na koszt tworzenia stanów w terminach bezpieczeństwa.

Od kilkunastu lat trwają nieustanie prace nad wdrożeniem kwantowego Internetu – sieci kwantowej która umożliwiłaby między innymi bezpieczną komunikację i kwantowe obliczenia w chmurze w skali między-kontynentalnej, w odróżnieniu od obecnych komercyjnych połączeń z punktu do punktu w skali metropolitalnej i kontynentalnej. W oczekiwaniu na przełom technologiczny który pozwoli wdrożyć ideę kwantowego Internetu chcemy w ramach niniejszego projektu ocenić koszt różnych jego realizacji w terminach bezpiecznego klucza. Trzeci cel projektu stanowi określenie czy w skali między-kontynentalnej ilość klucza kryptograficznego może przewyższać ilość ustalonego czystego splątania. W zależności od wyniku oszacowany zostanie koszt sieci kwantowej w skali międzykontynentalnej w terminach czystego splątania lub klucza kryptograficznego. Kolejnym podzadaniem będzie zbadanie kosztu połączeń umożliwiających bezpieczne rozmowy użytkowników sieci jak również postawienie analogicznych pytań dotyczących sieci kwantowej której bezpieczeństwo nie zależy od urządzenia.

Powyższy projekt badań, ma w dużej mierze charakter pionierski. Do przewidywanych jego efektów należeć będą nowe, bardziej ekologiczne sposoby przetwarzania danych kwantowych, znajomość najtańszego ze scenariuszów kryptograficznych w terminach bezpieczeństwa jak również oszacowanie kosztu kwantowego Internetu w terminach bezpiecznego klucza kryptograficznego. Przewidywany jest też rozwój wiedzy o zasobach kwantowych. Szersza wizja tego projektu obejmuje nie tylko badanie kosztu stanów kwantowych oraz zasobów związanych ze stanami, lecz również koszt kwantowych kanałów komunikacyjnych.