Informatyka kwantowa zajmuje się badaniem zastosowania mechaniki kwantowej w przetwarzaniu, przechowywaniu i przesyłaniu informacji. Najbardziej spektakularnym zastosowaniem technologii kwantowych w informatyce jest kryptografia kwantowa. W dzisiejszych czasach istnieją już komercyjnie systemy kwantowe do szyfrowania oraz przesyłania wiadomości. Kryptografia kwantowa przedstawia nowy rodzaj bezpieczeństwa i jedyne założenie to, że mechanika kwantowa jest poprawnym opisem rzeczywistości. Nie ma żadnych założeń dotyczących strony podsłuchującej, wystarczy aby nie łamała praw mechaniki kwantowej. Bezpieczeństwo kwantowych protokołów kryptograficznych może być wówczas udowodnione.

Niestety przy konkretnych realizacjach protokołów kryptograficznych pojawiają się zakłócenia, które powodują, że działanie protokołu różni się w pewien sposób od założonego protokołu. Kluczowym zagadnieniem w tym momencie jest oszacowanie w jakim stopniu zakłócenia, spowodowane przez nieidealną implementację protokołu, wpływają na bezpieczeństwo całego systemu. Pojawienie się zakłóceń – szumów, modeluje się za pomocą tzw. kanałów kwantowych. Badając sytuację ogólną, nie narzuca się żadnych założeń co do rodzaju szumów i modeluje się kwantową linię komunikacyjną jako pewną mieszankę linii idealnej – nie zmieniającej przesyłanego stanu, oraz losowego szumu modelowanego jako losowy kanał kwantowy.

Aby zbadać własności w/w mieszanki należy przede wszystkim zrozumieć własności losowych i typowych kanałów kwantowych. W ramach projektu badane będą własności teorio-informacyjne typowych kanałów, dzięki którym będzie można ocenić bezpieczeństwo typowej linii komunikacji kwantowej.