Ważnym odkryciem w teorii szyfrowania jest kryptografia z kluczem publicznym. W protokołach tego typu każda ze stron posiada parę kluczy: prywatny oraz publiczny. Klucz publiczny może być znany dowolnej stronie, która może za jego pomocą przesłać wiadomość do posiadacza klucza. W 1977 roku Rivest, Adleman oraz Shamir odkryli kryptografię z kluczem publicznym, przedstawiając protokół kryptograficzny znany jako RSA. Bezpieczeństwo RSA oparte jest o założenie, że rozkład liczby złożonej na czynniki pierwsze jest zadaniem czasochłonnym obliczeniowo. W roku 1984 powstała kolejna metoda szyfrowania, ElGamal. Bezpieczeństwo tej metody oparte jest na założeniu, że wyznaczenie logarytmu dyskretnego jest zagadnieniem złożonym obliczeniowo. Istnieją również protokoły kryptograficzne z kluczem publicznym oparte o krzywe eliptyczne nad ciałami skończonymi odkryte w 1985 roku przez Koblitza oraz Millera.

Podsumowując można stwierdzić, iż klasyczne schematy kryptograficzne oparte są na wymienionych poniżej założeniach
Założenie 1: moc obliczeniowa strony podsłuchującej jest ograniczona,
Założenie 2: rozkład liczb na czynniki pierwsze, wyznaczanie logarytmu dyskretnego itp. jest zadaniem złożonym obliczeniowo.

Potencjalne komputery kwantowe rzucają cień na długofalowe zastosowania wymienionych powyżej schematów kryptograficznych. Przykładowo algorytm Shora jest w stanie wykonać efektywnie rozkład na czynniki pierwsze, a także wyznaczyć logarytm dyskretny na krzywych eliptycznych.

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.

Celem projektu jest przeprowadzenie dowodu bezpieczeństwa kwantowych protokołów wymiany klucza z uwzględnieniem najbardziej ogólnego rodzaju ataku, tj. zakładając że strona podsłuchująca ma dostęp do pamięci kwantowej oraz może w pewnym stopniu splątać swój system z transmitowanym kubitem. W tym celu wyznaczona zostanie uniwersalna warunkowa entropowa relacja nieoznaczoności oraz stworzony zostanie formalizm, oparty o uogólnione teorie probabilistyczne, umożliwiający analizę bezpieczeństwa kwantowych protokołów wymiany klucza.