dr Anna Kamińska
Dyrektor Pionu QS
Creotech Instruments S.A

„Polskie komercyjne systemy kwantowej dystrybucji klucza szyfrującego”

Standardowe, obecnie stosowane protokoły wymiany kluczy publicznych opierają się na asymetrycznych algorytmach szyfrowania, takich jak RSA, w celu ustanowienia kluczy sesji i zapewnienia bezpieczeństwa komunikacji. Szyfrowanie asymetryczne należy do kategorii bezpieczeństwa obliczeniowego, opartego na założeniu, że zasoby obliczeniowe przeciwnika są niewystarczające do przeprowadzenia kryptoanalizy lub łamania brute-force. Takie bezpieczeństwo, nieoparte na żadnym ścisłym dowodzie, może zostać złamane przez nowe podejścia obliczeniowe lub dostępne w niedalekiej przyszłości komputery kwantowe implementujące algorytm Shora.

Innym, aktualnie najbardziej nowoczesnym podejściem jest kwantowa dystrybucja klucza (Quantum Key Distribution, QKD) opartego na bezpieczeństwie teorioinformacyjnym, które można udowodnić w oparciu o podstawowe prawa fizyki. QKD jest zupełnie nową technologią ustanowienia klucza szyfrującego, której implementacja wymaga dedykowanych urządzeń i ich integracji w istniejącej infrastrukturze.

W niniejszym wystąpieniu zaprezentowana zostanie istota technologii QKD oraz nowy produkt polskiej spółki Creotech – system QKD, umożliwiający implementację tej technologii w istniejących infrastrukturach telekomunikacyjnych opartych o sieci światłowodowe.