Historia szyfrowania informacji jest tak samo stare jak historia ich wymiany.
Próbowano zaszyfrować przesyłane dane tak, aby nie przedostały się one w niepowłane ręce.
Zależały od tego losy wojen, a także losy nie jednej miłosnej relacji.
Proste szyfry mono i polialfabetyczne maszyna Lorenza, czy chociażby legendarna enigma to już jedna historia.
Obecnie większość danych przesyłamy sieciami światłowodowymi wykorzystując do tego światło jego wyjątkowe własności fizyczne, a zaawansowane klucze kryptograficzne zabezpieczają strategiczne dane,
między innymi choćby strony internetowe czy transakcje bankowe.
Prostące możliwości obliczeniowe systemów próbujących wykraść cenne informacje,
a także rozwój tak zwanych komputerów kwantowych to wszystko zmieniło zasady gry.
Bojawia się pole dla kryptografii kwantowej, która dotychczasowe podejście do bezpiecznej komunikacji wywraca do góry nogami.
Dotychczas szyfrowanie było trochę zamkniętym kołem, taką zabawą w kotka i myszkę,
opracowaniem szyfru, a potem wymyśleniem sposobu na złamanie go.
Skutkowało to pracami nad kolejnym szyfrem, co owocowało kolejną próbą złamania.
Kryptografia kwantowa diametralnie zmienia te zasady gry, bo na scenę weszła fizyka.
W pewnym uproszczeniu można powiedzieć, że kwantowa kryptografia wykorzystuje prawa fizyki, a kryptografia klasyczna prawa matematyki.
Fizyka opisuje właściwości, zjawiska, oddziaływania.
Matematyka daje nam do tego narzędzia, daje narzędzia do wnioskowania,
jest językiem opisu zjawisk obserwowanych dzięki fizyce.
Złamanie kwantowego klucza, czy kwantowo wymienionego klucza kryptograficznego
wiązałoby się nie tyle między złamaniem jakiegoś konkretnego szyfru,
ale ze złamaniem praw fizyki.
Z punktu widzenia obecnej wiedzy jest to po prostu niemożliwe.
Kryptografia kwantowa z uwagi na prawa fizyki i dowody matematyczne,
które za nią stoją, daje nam więc pewność, co do jej metod.
Wszak podstawy fizyki teoretycznej rozmaite teorie kwantów
zostały udokumentowane i nagrodzone wieloma nagrodami Nobla.
Zresztą nagroda Nobla z fizyki w roku 2022
została przyznana trzem naukowcom właśnie za pracę nad splątaniem kwantowym.
Myślę, że najciekawszym zagadnieniem w dziedzinie kryptografii kwantowej
jest kwantowa dystrybucja klucza, czyli QQD.
Jeśli ktoś, kto chce przechwycić nasze dane
albo klucz zajrzy do systemu, będziemy o tym wiedzieć.
Problemem łamania kluczy kluczy kryptograficznych
jest fakt, że mogą one zostać złamane bez wiedzy
stron wymieniających się informacjami.
Można używać narzędzi, nie wiedząc, że są już one bezużyteczne.
Niemcy używali enigmy, bo nie mogli wiedzieć,
że zasady jej działania już została nomenomen odszyfrowana.
W przypadku kryptografii kwantowej to wszystko działa zupełnie inaczej.
To co stoi u podstaw tego bezpieczeństwa

to nic innego jak fundamenty mechaniki kwantowej.
QQD wykorzystuje właściwości pojedynczych fotonów,
czyli kwantów energii świetlnej.
Istotą kwantowego podejścia jest umiejętność kontrolowania pojedynczych fotonów,
atomów albo stanów kwantowych światła i materii.
Kluczem do zrozumienia, czym jest ta kwantowa dystrybucja klucza
jest uświadomienie sobie, że zadaniem QQD nie jest transmisja danych
i wiadomości, a stworzenie i dystrybucja klucza kryptograficznego,
czyli narzędzia, dzięki któremu można zasyfrować
albo odszyfrować przesłane dane.
QQD jest więc zestawem procedur, technologią,
która umożliwia wymiany klucza kryptograficznego
między zainteresowanymi stronami w bezpieczny sposób,
bez możliwości skopiowania go i odczytania przez osoby postronne.
Na system, oprócz odbiorcy i nadawcy składa się kanał klasyczny
do przesyłania informacji oraz kanał kwantowy,
którym przesyłany jest klucz kryptograficzny.
W kanale klasycznym nośnikiem informacji może być dowolny sygnał.
Natomiast w przypadku kanału kwantowego
informacja wysyłana jest za pomocą pojedynczych kwantów światła.
Każdy z tych kwotonów ma losowy stan kwantowy,
pionową albo poziomą polaryzację.
Nie wchodząc za bardzo w madry fizyki kwantowej,
określamy te stany jako 1 lub 0.
Odbiornik z kolei możemy ustawić tak,
aby odróżniał te pionowe i poziome polaryzacji od siebie.
Tak jak najmniejsze porcje informacji nazywamy bitami,
tak najmniejsze jednostki informacji kwantowej
nazywamy kubitami od quantum bit, kwantowych bitów.
W kwantowej dystrybucie klucza mamy
swoistą zmianę sposobu myślenia o bezpieczeństwie.
Nie zastanawiamy się nad wymyślnymi matematycznymi zabezpieczeniami,
czy kodami tylko patrzymy,
czy cała komunikacja zaszła z zachowaniem bezpieczeństwa.
A jeśli mamy jakąkolwiek wątpliwość,
po prostu nie używamy klucza,
który wygenerowaliśmy w danej rundzie.
Przykładowo w protokole BB84 wysyłamy klucz bez żadnych zabezpieczeń,
ale możemy sprawdzić, czy ktoś spojrzał na niego po drodze.
Jeżeli ktoś nas podsłuchuje, bezpiecznego klucza w ogóle nie uda się ustalić.
Nie da się pasywnie podsłuchiwać bez szkody dla klucza.
Odwracają sytuację, jeśli ustalimy klucz,
to mamy gwarancję, że nikt nas nie podsłuchał.
Ideę QQD testuje się i wdraża na wiele różnych sposobów.

Polscy fizycy również mogą pochwalić się dużymi zasługami.
Między Poznaniem a Warszawą testowane jest najdłuższe łącze QQD w Europie.
Obecnie prowadzone są różnorodne badania nad integracją systemu
tego kwantowego z infrastrukturą już istniejącą,
a także nad możliwościami wykorzystania tej technologii
w rozmaitych aplikacjach i usługach.
Polski fizyk Artur Eckert jest autorem jednego z najważniejszych protokołów QQD E91.
Protokół ten wykorzystuje splątane pary fotonów i łamanie nierówności Bella.
Rozwiązania kwantowe w kryptografii już są,
albo będą używane przede wszystkim do chronienia infrastruktury krytycznej.
To co warto zapamiętać z dzisiejszego odcinka to fakt,
że nie jest możliwe, żeby kryptografia kwantowa zastąpiła kryptografię taką konwencjonalną klasyczną.
Bo inny de facto jest faktyczny cel kryptografii kwantowej,
której rola polega na stworzeniu i dystrybucji klucza kryptograficznego,
czyli narzędzia do szyfrowania danych.
Oba podejścia klasycznej kwantowe będą więc funkcjonować obok siebie
jako swoiste podwójne zabezpieczenie.
Wykorzystując w kryptografii technologie kwantowe
zaprzęgamy do pracy fundamentalne prawa fizyki
i to jest najlepsza gwarancja niezawodności tych technologii.
Tak jak grawitacja gwarantuje nam, że nie zaczniemy lewitować,
tak fizyka kwantowa zastosowana w kryptografii gwarantuje nam,
że nasze dane nie zostaną przejęte przez niepożądaną osobę czy organizację.
Nauka to lubię od 10 lat, nie tylko na Facebooku i YouTube.