Kryptokwanty

Kto i kiedy wymyślił szyfrowanie, tego nikt nie wie. Może Egipcjanie, może Fenicjanie, a może ktoś inny. Gdzieś w basenie Morza Śródziemnego, jakieś 500 lat p.n.e. ktoś wpadł na pomysł, że można przestawiać litery i modyfikować tekst tak, że przeczyta go tylko osoba wtajemniczona. Wiemy, że dosyć prostymi szyframi posługiwali się już starożytni Grecy i Rzymianie. Z czasem wymyślono coraz bardziej wyszukane metody i zaczęto zawierzać tajemnice korespondencji matematyce. Problem w tym, że za każdym genialnym pomysłem matematycznym stał do tej pory inny, równie genialny pomysł matematyczny, który pozwalał te szyfry łamać. Warto tu wspomnieć chociażby historię Enigmy. Dzisiaj jednak wiemy, że można zaprojektować szyfr doskonały, ale wymaga on bezpiecznej dystrybucji dużej ilości zupełnie przypadkowych bitów, z których później konstruuje się tajne teksty. Te przypadkowe bity to tzw. klucz kryptograficzny.

Szyfr doskonały, z kluczem jednorazowym, jest w miarę prosty. Jeśli nadawca i odbiorca są w posiadaniu tego samego ciągu losowo wygenerowanych zer i jedynek – czyli klucza — to nadawca najpierw zapisuje tekst depeszy w postaci binarnej, używając powszechnie znanego kodu ASCII, gdzie A=01000001, B=01000010, etc., a następnie dodaje każdy bit depeszy do odpowiedniego bitu klucza (dodawanie binarne to takie, w którym 0+1=1+0=1, a 0+0=1+1=0. Tak więc, jeśli tekst depeszy zaczyna się od 01000001…, a klucz od 01101111…, to pierwsze osiem bitów szyfru to 00101110. Szyfr niejako dziedziczy przypadkowość po kluczu, dodanie depeszy, w której bity bynajmniej nie są przypadkowe, do losowo generowanego klucza, daje szyfr, w którym bity są zupełnie przypadkowe. Nadawca może teraz wysłać szyfr drogą radiową. Każdy może monitorować te transmisje i odczytać wszystkie bity szyfru, ale tylko odbiorca – drugi posiadacz klucza – jest w stanie odczytać depesze, dodając bit po bicie, szyfr do klucza (jak łatwo sprawdzić, w dodawaniu binarnym suma dwóch identycznych liczb daje zero, więc działanie to usuwa klucz z szyfru i pozostaje sama depesza). Można udowodnić, że jeśli klucz jest zupełnie losowy, tajny, ma tyle samo bitów co depesza i jest użyty tylko jeden raz, to szyfru takiego złamać się nie da.

Pozostaje „drobiazg”: jak bezpiecznie wygenerować klucz, czyli losowe bity, na odległość? Nie jest to łatwe.

Matematycy wymyślili kilka genialnych metod obejścia problemu. W latach siedemdziesiątych ubiegłego wieku wynaleziono tzw. szyfry z kluczem publicznym; metody te bazują na teorii złożoności procesów obliczeniowych, tzn. zakłada się, że niektóre problemy matematyczne, np. rozkład dużych liczb na czynniki pierwsze, są trudne do rozwiązania. Niestety, jakie problemy są naprawdę trudne nie jest jasne i nikt nie wie czy oprą się one nowym algorytmom. Tak więc równie trudno jest udowodnić, że szyfry z kluczem publicznym sa bezpieczne.

Mniej więcej w tym samym czasie kiedy wymyślono szyfr doskonały, na początku XX wieku, fizycy zaczęli deliberować na przypadkowością w nowo powstałej mechanice kwantowej. Najpierw Einsteinowi nie podobało się, że w ogóle jest jakaś przypadkowość, potem innym nie podobało się, że Einsteinowi się coś nie podobało, i wymianie argumentów zdawało się nie być końca. Z jednej strony mechanika kwantowa przewidywała tzw. splątanie kwantowe — obiekty oddalone lata świetlne od siebie nadal zachowywały się tak, jakby jeden wiedział, co dzieje się z drugim, i dawały te same wyniki podczas pewnych pomiarów. Z drugiej strony przypadkowość tych wyników nie pozwalała na wykorzystanie splątania do natychmiastowej, nadświetlnej komunikacji. Aby przesłać informacje, np. jeden bit, musimy najpierw wybrać, czy chcemy przesłać 0 czy 1, splątanie kwantowe nie daje nam możliwości takiego wyboru. Kiedy mierzymy splatane bity, zwane qubitami, wyniki są identyczne, ale przypadkowe — my nie mamy wpływu na wynik, więc nie możemy sobie wybrać 0 czy 1.

Dysputy miały charakter raczej filozoficzny, dopóki John Bell – pracujący w CERN-ie fizyk z Belfastu — nie pokazał, że pewne kwestie można rozstrzygnąć na drodze eksperymentalnej. W szczególności można weryfikować bezwzględną nieprzewidywalność wyników pomiarów na splątanych obiektach. Oznacza to, że jest pewien test, który może wykazać, że nikt, absolutnie nikt, nie jest w stanie przewidzieć wyników pomiarów, zanim pomiary te zostaną przeprowadzone.

Cóż to oznacza dla kryptologów? Ano to, że można zweryfikować, iż przypadkowe bity – np. wyniki pomiarów na splątanych fotonach przeprowadzone w dwóch odległych miejscach – są tajne, czyli nieprzewidywalne przez nikogo. Stąd już blisko do bezpiecznej dystrybucji klucza kryptograficznego. Klucz nie niesie w sobie żadnej informacji – to zupełnie przypadkowy ciąg bitów – ale na jego bazie buduje się później tajną korespondencję. Aby zamienić intuicję w coś bardziej konkretnego, trzeba było dodać trochę matematyki, trochę oszacowań, z dużą ilością delt i epsilonów, i w końcu udało mi się udowodnić, że test Bella dotyczący podstaw mechaniki kwantowej przydaje się również do weryfikacji bezpieczeństwa klucza kryptograficznego. Jak każdy teoretyk, przyglądałem się z niedowierzaniem pierwszym doświadczeniom przeprowadzonym przez moich kolegów Johna Rarity’ego i Paula Tapstera, pracujących dla brytyjskiej Defence Research Agency; wyniki pokazały jednak, ponad wszelką wątpliwość, że to naprawdę działa!

Dzisiaj kryptografia kwantowa to najbardziej zaawansowana dziedzina nowych technologii kwantowych. Satelity, takie jak np. chiński Micius, wysyłają splątane fotony do odległych o tysiące kilometrów stacji naziemnych i pozwalają na bezpieczną generację klucza. Europa i Stany Zjednoczone budują kwantowy internet. Szyfry, których nie da się złamać, stają się rzeczywistością. A co dalej? Przyszłość nigdy nie jest taka, jak nasze przewidywania, ale bez wątpienia kryptografia, a wraz z nią mechanika kwantowa, będzie odgrywać coraz bardziej istotną rolę w naszym życiu i w ochronie naszej prywatności. Dla mnie ta cała historia — od filozoficznej debaty na temat przypadkowości w mechanice kwantowej do tajnej transmisji danych — pokazuje, iż warto inwestować w badania podstawowe. Nigdy nie wiadomo, co nam się wykluje z tych abstrakcyjnych równań.

ARTUR EKERT
University of Oxford