opierać się komputerom kwantowym. W roku 2015 NSA wezwała do przejścia na algorytmy odporne na komputery kwantowe opracowane tak, aby były bezpieczne, nawet gdy te się pojawią. W roku 2017 amerykańska agencja standaryzacji NIST zaczęła proces, który w rezultacie powinien doprowadzić do standaryzacji algorytmów postkwantowych.

W tym rozdziale można więc znaleźć nietechniczny przegląd zasad, które spełniają komputery kwantowe, a także trochę informacji o algorytmach postkwantowych. Jest tu trochę matematyki, ale nic ponad podstawową arytmetykę i algebrę liniową, więc nie należy się obawiać trudnych notacji.

Jak działają komputery kwantowe

Komputery kwantowe to model obliczeniowy, który wykorzystuje fizykę kwantową, aby inaczej prowadzić obliczenia i wykonywać działania, jakich nie umieją robić klasyczne komputery, na przykład skuteczne złamanie RSA i kryptografii krzywych eliptycznych. Ale komputer kwantowy to nie jest superszybki zwykły komputer. W istocie komputery kwantowe nie potrafią rozwiązać żadnego problemu, który jest za trudny dla klasycznego komputera, jak poszukiwanie brutalne lub problemy NP-zupełne.

Komputery kwantowe są oparte na mechanice kwantowej, gałęzi fizyki badającej zachowanie cząstek subatomowych, które zachowują się naprawdę losowo. W przeciwieństwie do zwykłych komputerów, które działają na bitach i mają wartość 0 lub 1, komputery kwantowe są oparte na *bitach kwantowych* (*quantum bits* lub inaczej *kubity*), które jednocześnie mogą mieć wartość 0 i 1 – stan dwuznaczności zwany *superpozycją*. Fizycy odkryli, że w tym mikroskopowym świecie cząstki, takie jak elektrony i fotony, zachowują się w sposób wysoce nieintuicyjny: zanim zaobserwujemy elektron, nie znajduje się już on w określonym miejscu przestrzeni, lecz w kilku miejscach w tym samym czasie (czyli jest w stanie superpozycji). Ale gdy dokonamy obserwacji – działania nazywanego w fizyce kwantowej *pomiarem* – zatrzymuje się on w ustalonym losowym miejscu i przestaje znajdować się w superpozycji. Ta magia kwantowa pozwala na tworzenie kubitów w komputerze kwantowym.

Ale komputery kwantowe działają tylko dlatego, że istnieje jeszcze bardziej zwariowane zjawisko zwane *splątaniem* – dwie cząstki mogą być połączone (splątane) w taki sposób, że obserwacja wartości jednej z nich daje nam wartość drugiej, jeśli nawet dwie cząstki są daleko od siebie (kilometry lub nawet lata świetlne od siebie). To zachowanie zostało zilustrowane przez *paradoks EPR* (*Einstein–Podolsky–Rosen*) i jest powodem, dla którego Albert Einstein na początku odrzucił mechanikę kwantową (szczegółowe wyjaśnienie można znaleźć na stronie *https://plato.stanford.edu/entries/qt-epr/*).

Aby najlepiej wytłumaczyć działanie komputera kwantowego, musimy odróżnić rzeczywisty komputer kwantowy (sprzęt złożony z bitów kwantowych) od algorytmów kwantowych (oprogramowania, które na nim działa, złożone z *bramek kwantowych*). Dwa poniższe punkty omawiają te dwa pojęcia.