14

KRYPTOGRAFIA KWANTOWA I POSTKWANTOWA

W poprzednich rozdziałach tematem była dzisiejsza kryptografia, natomiast w tym rozdziale przeanalizujemy przyszłość kryptografii w horyzoncie czasowym, powiedzmy 100 lub więcej lat – w czasie, gdy będą istniały *komputery kwantowe*. Komputery kwantowe to komputery wykorzystujące fizykę kwantową w celu wykonywania innego rodzaju algorytmów niż te, do których jesteśmy przyzwyczajeni. Komputery kwantowe jeszcze nie istnieją i wygląda na to, że są trudne do zbudowania, ale jeśli kiedyś zaistnieją, będą miały potencjał do złamania RSA, Diffiego–Hellmana i kryptografii krzywych eliptycznych – czyli całej wdrożonej kryptografii klucza publicznego i standardów znanych w chwili pisania tej książki.

Aby zabezpieczyć się przed ryzykiem stwarzanym przez komputery kwantowe, badacze kryptografii opracowali alternatywne algorytmy kryptograficzne klucza publicznego, zwane algorytmami postkwantowymi, które będą