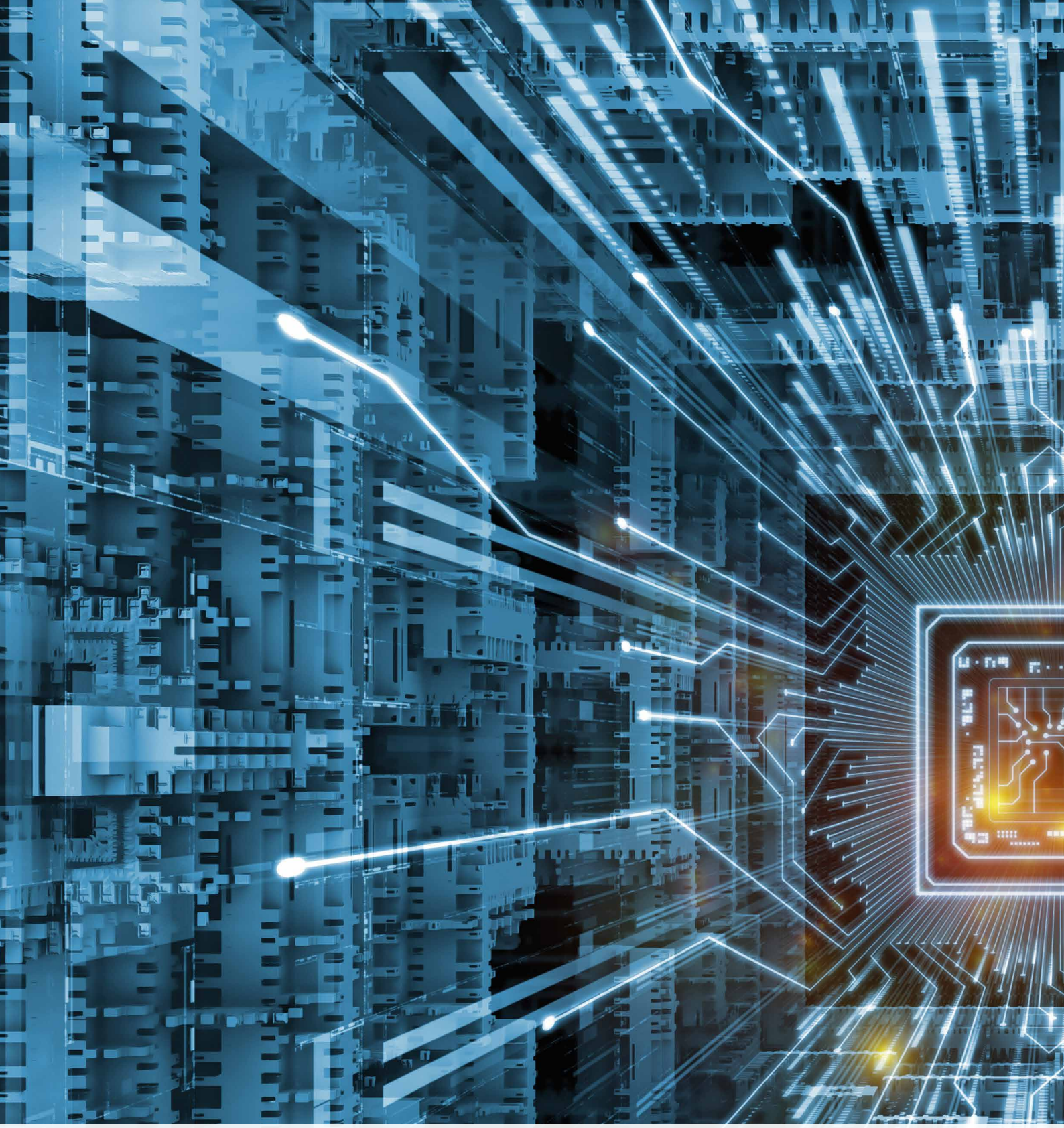
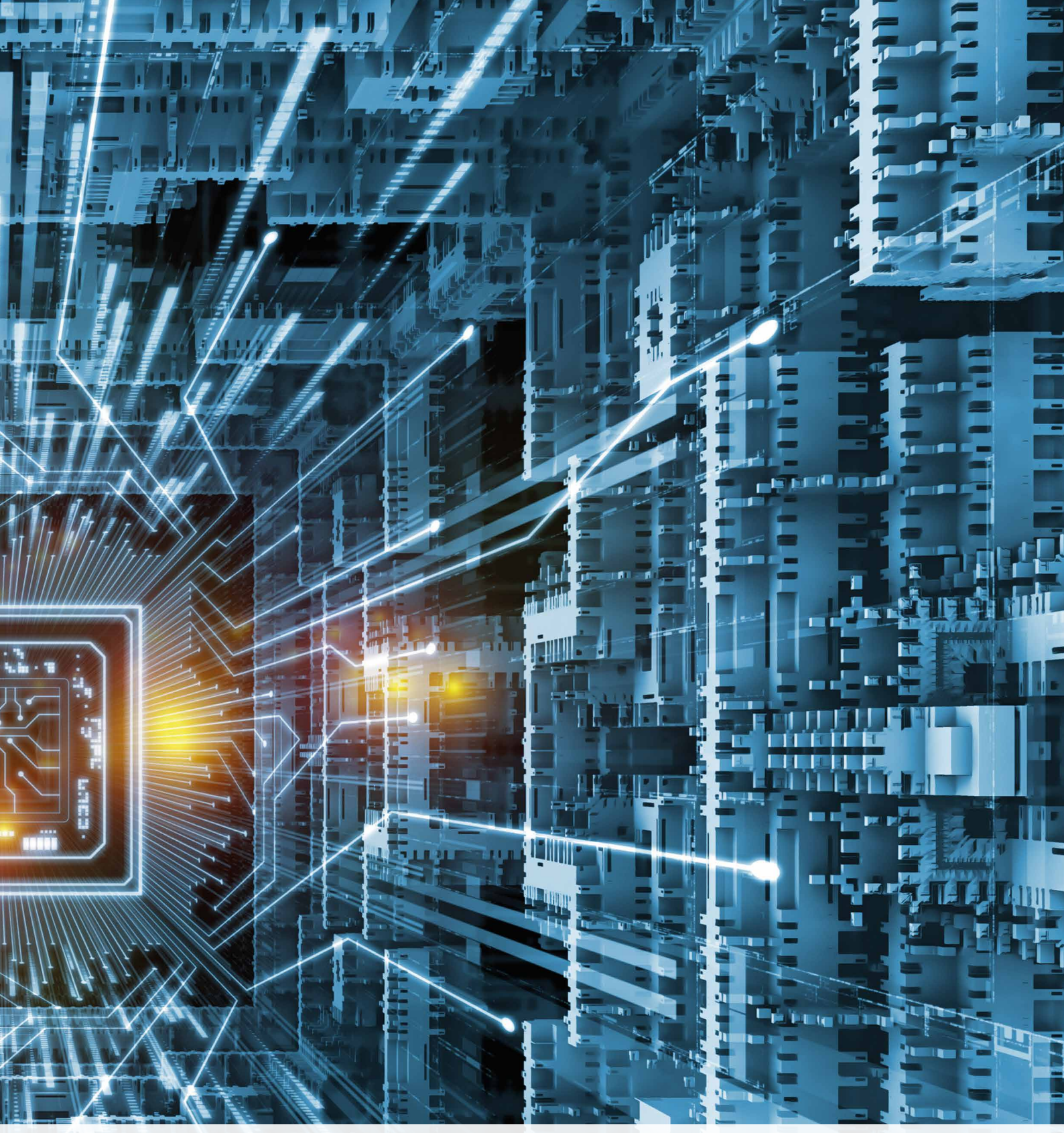


KWANTOWE ATAKI NA KLA

Rys. Andrew Ostrovsky



ASYCZNE KRYPTOSYSTEMY

Zaczęło się od eksperymentu myślowego w 1970 roku, gdy fizyk Stephen Wiesner wpadł na pomysł, by klasyczne zabezpieczenia banknotów zastąpić kwantowymi. Nowatorska idea musiała jednak poleżeć parę dekad w szufladzie, zanim dało się jej założenia przetestować eksperymentalnie.

W kwantowych pieniądzach zamiast unikatowych numerów seryjnych nadrukowanych na banknotach i widocznych dla każdego gołym okiem S. Wiesner chciał wykorzystać właściwości cząstek elementarnych, jak polaryzacja czy spin. Wówczas tylko za pomocą odpowiednio skonstruowanej aparatury istniałaby możliwość odczytania naniesionego kodu. Takich pieniędzy nie dałoby się też podrobić. Eleganckie rozwiązanie było jednak poza możliwościami ówczesnej techniki.

Podejmowane w tamtym czasie eksperymenty pozwalały mimo wszystko żywić nadzieję, że pomysł da się zastosować w praktyce. W latach 80. ubiegłego wieku rozważano wykorzystanie w kryptografii kwantowej pojedynczych kubitów (w informatyce kwantowej kubit jest odpowiednikiem bitu w informatyce klasycznej; w odróżnieniu od bitu, który przyjmuje jedynie wartość 1 albo 0, kubit może znajdować się w stanie superpozycji dwóch stanów kwantowych, w uproszczeniu będących jednocześnie 1 i 0), a w 1991 roku polski naukowiec Artur Ekert zaproponował zastosowanie w tym celu ich stanów splątanych. Przeprowadzone cztery lata później doświadczenia zespołu, w którego skład wchodził Anton Zeilinger – światowy autorytet w dziedzinie informacji kwantowej – dowiodły, że faktycznie można to zrobić. Zanim jednak rozwiniemy wątek kryptografii, musimy przyjrzeć się samym komputerom kwantowym.

POTĘGA KOMPUTERA KWANTOWEGO

Praktycznie nie ma dnia, w którym przeglądając różne portale, nie natrafimy na krzykliwy nagłówek obwieszczający: *Przełom w rozwoju komputerów kwantowych!* Zapytany o to, ile w szumnych doniesieniach mediów jest prawdy, prof. dr hab. Jerzy Dajka, fizyk z Uniwersytetu Śląskiego, odpowiada:

– Ciągle jesteśmy daleko od zrobienia czegoś, co by było praktycznie dostępne. Nie najlepiej radzimy sobie z dekoherencją, czyli utratą informacji w wyniku oddziaływania układu z otoczeniem. Wciąż też mamy za mało kubitów. Te eksperymenty, o których wiemy, wydają się dowodzić, że osiągnęliśmy przewagę kwantową dla pewnych stosunkowo prostych zagadnień. Pojawia się jednak kwestia rozmiaru. Rzeczywiście, jesteśmy w stanie dokonać czegoś prostego za pomocą kubitu szybciej niż dla bitów, ale jeżeli mamy zagadnienie, które wymaga zakodowania czegoś za pomocą dziesiątek tysięcy bitów klasycznych, to jeszcze nie dysponujemy tyloma kubitami, by z tym powalczyć. Nadal jesteśmy na etapie wstępnym i bardziej teoretycznym, jeżeli chodzi o obliczenia kwantowe.

Obecnie posiadaniem stale rozwijanych komputerów kwantowych mogą się pochwalić amerykańskie przedsiębiorstwa IBM (Quantum) i Google (Quantum AI), a także kanadyjskie D-Wave Systems. Przy czym to ostatnie specjalizuje się w pewnej klasie algorytmów, za pomocą których rozwiązać może dość wąski zakres problemów.

– Jakkolwiek D-Wave wydaje się technologicznie najbardziej zaawansowany, to paradoksalnie stanowi najmniejsze zagrożenie dla klasycznej kryptografii – przekonuje naukowiec. – A na czym to zagrożenie polega?

OBNAŻAJĄC INFORMACJĘ

Przypomnijmy sobie wspomniane wcześniej kwantowe pieniądze S. Wiesnera. W wielu dziedzinach bowiem korzystamy z różnego rodzaju szyfrów i kodów mających za zadanie chronić nasze dane. Czy dotyczy to konta bankowego, profilu pacjenta w systemach służby zdrowia, albo tajemnic wojskowych lub gospodarczych – wszędzie nad bezpieczeństwem informacji czuwają różnego rodzaju algorytmy stosowane w kryptografii klasycznej.

Często nie mamy pewności, czy nie da się ich złamać. Wiemy tylko, że nie jesteśmy w stanie zrobić tego w czasie krótszym niż czas życia Wszechświata. Chyba że ktoś próbujący przebić się przez taki algorytm będzie dysponował komputerem kwantowym.

– Taka osoba potrafiłaby złamać szyfr od razu. Świat zrobiłby się jednostronnie przezroczysty, to znaczy osoba z komputerem kwantowym widziałaby wszystkie dane zaszyfrowane klasycznymi metodami, ale druga strona nie miałaby dostępu do danych zabezpieczonych za pomocą kwantowych kryptosystemów – wyjaśnia prof. Jerzy Dajka.

Weronika Cygan

prof. dr hab. Jerzy Dajka
Instytut Fizyki
Wydział Nauk Ścisłych i Technicznych
Uniwersytet Śląski
jerzy.dajka@us.edu.pl

Wystarczy spojrzeć na opanowaną wojną Ukrainę, by uświadomić sobie, jak ogromne znaczenie ma informacja. Po inwazji na sąsiada Rosjanie w pierwszej kolejności niszczyli m.in. infrastrukturę komunikacyjną, by przeciwnik nie mógł się porozumiewać, ale też by odciąć go od wieści z frontu i uniemożliwić przesyłanie własnych komunikatów światu zewnętrznemu.

– Obecność w Ukrainie Starlinka od Elona Muska jest czynnikiem nietrywialnym. Udostępniając bowiem zaatakowanemu państwu swój telekomunikacyjny system satelitarny, biznesmen wizjoner sprawił, że tamtejsze wojsko i administracja nie są już w żaden sposób uzależnione komunikacyjnie od rosyjskich interwencji – tłumaczy fizyk.

Łatwo się zatem domyślić, że państwo, które jako pierwsze stworzy komputer kwantowy zdolny do wykonywania takich obliczeń, będzie dysponowało niebezpieczną bronią. Byłaby to dominacja w świecie, porównywalna jedynie do tej, jaka zaistniała po skonstruowaniu przez Amerykanów bomby atomowej. Trwała ona do czasu, gdy bomba pojawiła się również po drugiej stronie żelaznej kurtyny.

POSTKWANTOWA ZBROJA

Taki scenariusz brzmi dość groźnie, ale już teraz dysponujemy skuteczną ochroną przeciw kwantowym atakom na klasyczne kryptosystemy, w dodatku niewymagającą kwantowego komputera!

Protokoły postkwantowe, bo o nich mowa, opierają się na klasycznej infrastrukturze i od 2015 roku są rekomendowane przez amerykańską Narodową Agencję Bezpieczeństwa (NSA) jako sposób na potencjalne ataki ze strony komputerów kwantowych. Takie rozwiązania już się zresztą stosuje (m.in. przy „kopaniu" bitcoinów) i są one wysoce skuteczne.

W klasycznej kryptografii pewna grupa algorytmów opiera się na faktoryzacji liczb, czyli rozkładaniu ich na czynniki pierwsze – nawet jeśli wiemy, że liczba jest iloczynem dwu liczb pierwszych, to w przypadku dostatecznie dużych liczb nie potrafimy łatwo ich wskazać. Znane podejścia są bliskie metodzie prób i błędów. Przy wystarczająco dużej liczbie podejść w końcu jednak uda nam się znaleźć prawidłową odpowiedź. W złożonych przypadkach znalezienie odpowiedniego rozwiązania klasycznym sposobem mogłoby zająć miliony lub miliardy lat. Komputer kwantowy podobną łamigłówkę rozgryzie w mgnieniu oka, dlatego trzeba było znaleźć inny sposób zabezpieczeń.

Obecnie znany jest jeden kwantowy algorytm (i jego modyfikacje) mogący zagrozić klasycznym kryptosystemom: algorytm Shora, który służy faktoryzacji liczb. Zastosowanie klasycznego kryptosystemu nieopierającego się na faktoryzacji liczb pozwoli zatem jeśli nie rozwiązać, to odsunąć problem w przyszłość. I taka jest rola kryptografii postkwantowej, przynajmniej do czasu, gdy pojawi się kolejny algorytm.

OKIEŁZNAĆ PRAWA NATURY

Myśli się też nad obejściem problemu zagrożenia ze strony komputerów kwantowych. Pewnym wyjściem jest przesyłanie tajnego klucza do szyfrowania i deszyfrowania za pomocą metod kwantowych i przy użyciu kwantowych kanałów komunikacyjnych. Na tym polu mamy już duże osiągnięcia, a sama metoda działa świetnie i jest niezwykle bezpieczna.

Sposób ten wydaje się mieć nad klasycznym przewagę z dwóch szczególnych powodów, a oba czerpią z fundamentalnych praw natury. Pierwszym jest kwestia układu kwantowego, który zmienia się zawsze podczas dokonywania pomiaru. Oznacza to, że przy odpowiednich narzędziach jesteśmy w stanie wykryć czyjąś ingerencję w informację. Po drugie – nie da się kwantowej informacji skopiować.

Choć wielu publicystów chętnie straszy komputerami kwantowymi mającymi stanowić wyzwanie dla bezpieczeństwa danych, wcale nie jesteśmy bezbronni w obliczu tego zagrożenia. Matematycy i informatycy wciąż udoskonalają obecnie wykorzystywane klasyczne kryptosystemy, jednocześnie fizycy pracują nad nowymi rozwiązaniami kwantowymi. Powinniśmy więc na komputery kwantowe patrzeć tak, jak patrzymy na nasze smartfony czy laptopy – są po prostu narzędziami, które można wykorzystać do różnych celów – i dobrych, i złych.