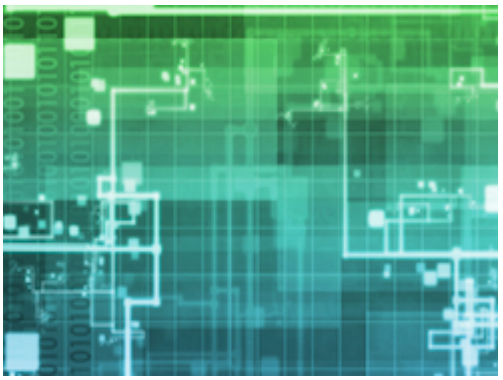
Zabezpieczanie szyfrowania danych przed przyszłym zagrożeniem ze strony komputerów kwantowych

Kiedy rozpowszechnią się komputery kwantowe, istniejący algorytm postawi pod znakiem zapytania obecne techniki szyfrowania, uważane teraz za bezpieczne. Prace realizowane w ramach finansowanego ze środków UE projektu kładą podwaliny pod rozwiązanie tego problemu.



© kentoh, Shutterstock

W artykule opublikowanym niedawno w czasopiśmie »Nature«, naukowcy opisują kilka podejść do opracowania nowych technik szyfrowania odpornych na ataki kwantowe. Jedną z oczywistych ścieżek jest stworzenie nowych technik szyfrowania, które nie korzystają z obecnych technologii, bo mogą się one nie sprawdzić w przyszłości.

Problem, w obliczu którego staje dzisiejsze szyfrowanie

Obecnie bezpieczeństwo online opiera się w dużej mierze na tzw. systemie RSA (Rivest-Shamir-Adleman), na którym bazuje szyfrowanie. System wykorzystuje klucze publiczne, składające się z iloczynu dwóch liczb pierwszych. Na dzień dzisiejszy nawet najsilniejszym komputerom sporo czasu zabrałoby zidentyfikowanie dwóch liczb pierwszych w procesie zwanym faktoryzacją. Najwydajniejszym superkomputerom rozwikłanie tej zagadki zajęłoby wieki.

Po drugiej stronie zaszyfrowanych danych jest adresat wiadomości, posiadający klucz prywatny w postaci liczby znanej tylko jemu oraz nadawcy. W drodze operacji matematycznej dwie liczby pierwsze wymagane do odkodowania wiadomości, uzyskiwane są za pomocą klucza prywatnego. Tak długo, jak klucz prywatny nie

zostanie przechwycony, szyfrowanie jest silne.

Jednak zbliżające się wielkimi krokami silne komputery kwantowe sprawią, że moc obliczeniowa potrzebna do skrakowania liczb pierwszych stanie się dostępna, przez co proces, który dotąd był dosyć szczelny, stanie się znacznie bardziej przepuszczalny. Wiadomo o tym od roku 1994, kiedy to opublikowany został algorytm komputera kwantowego, który rozdzieliłby duży klucz publiczny na dwie liczby pierwsze w ciągu sekund albo minut.

Naukowcy ustalają pierwsze etapy na drodze do rozwiązania

Zespół PQCRYPTO (Post-Quantum CRYPTOgraphyfor long-term security) nakreśla dwutorowe podejście: oprócz przekonania, że realne rozwiązanie może być oparte na stworzeniu nowych technik szyfrowania, innym pomysłem jest skoncentrowanie się na technikach wykorzystujących takie operacje matematyczne, z którymi komputery kwantowe nie dadzą sobie rady.

Naukowcy wskazują na kilka ograniczeń opracowywanych technik. Powinny one budzić zaufanie i nie być zbyt kosztowne we wdrożeniu ani zbyt wymagające pod względem systemów obliczeniowych. Należy też unikać kluczy o nadmiernej długości. Autorzy podkreślają jeden ważny aspekt opracowywania przyszłych post-kwantowych systemów szyfrowania: zwracanie od samego początku uwagi na standaryzację, ponieważ wszystkie strony będą musiały używać tych samych systemów kryptograficznych.

Więcej informacji:
witryna projektu PQCRYPTO

Kraje

Niderlandy

Powiązane projekty

PROJEKT

Post-quantum cryptography for long-term security

PQCRYPTO

7 Września 2023

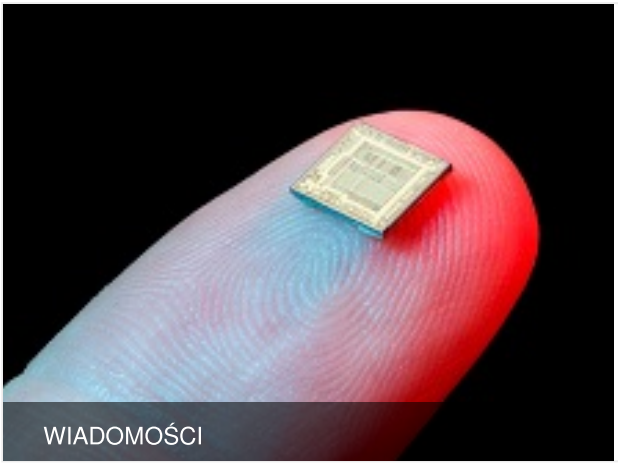
Powiązane artykuły

WIADOMOŚCI

POSTĘPY NAUKOWE

Czy można zapobiec cyberatakom komputerów kwantowych? Unijna inicjatywa pokazuje, jak tego dokonać

26 Marca 2020



WIADOMOŚCI

POSTĘPY NAUKOWE

Przełom w dziedzinie układów krzemowych: sprzężenie spinowo-fotonowe stało się rzeczywistością

27 Lutego 2018

POSTĘPY NAUKOWE

Zalety zjawisk kwantowych w analizie sieci biologicznych, społecznych i technologicznych

9 Lutego 2018

POSTĘPY NAUKOWE

Kwantowy skok w ultraprecyzyjnych pomiarach i kodowaniu informacji?

24 Listopada 2017

Ostatnia aktualizacja: 11 Października 2017

Permalink: https://cordis.europa.eu/article/id/122627-securing-encryption-data-against-the-threat-of-future-quantum-computers/pl