Dawid Szlachta
Wydział Polonistyki, KJOWPiB

Co by było fajnie mieć: kryptografia kwantowa

Kiedyś odległa i dostępna jedynie w nielicznych labolatoriach fizyków, dziś coraz bardziej powszechna – kryptografia kwantowa podbija świat. Jeszcze parenaście lat temu była mrzonką rodem z powieści typu *science fiction*, następnie budziła kontrowersje. Po dziesięciu latach od udostępnienia pierwszych komercyjnych usług sieciowych, korzystających z szyfrowania metodą kwantową rozmawiamy z prof. Andrzejem Dąbrowskim o plusach i minusach nowej technologii.

Panie profesorze, jeszcze dwadzieścia lat temu kryptografia kwantowa wydawała się odległym marzeniem. Teraz możemy z niej korzystać codziennie.

To prawda. Choć początki kwantowej kryptografii sięgają lat dziewięćdziesiątych ubiegłego wieku (można było wtedy budować sieci kwantowe o zasięgu dziesięć kilometrów w przypadku światłowodu oraz niecałe dwa kilometry korzystając z połączeń bezprzewodowych), to rozwiązanie pewnych problemów technicznych, jak utrata dużej ilości fotonów, zajęło sporo czasu. Pamiętam, że u swoich początków ta technologia, mimo że obiecująca, nie liczyła się jakoś specjalnie wśród metod kryptograficznych. Ale czasy się zmieniają *(śmiech)*.

Zmieniły się czasy i zmieniły się technologie – pokonaliśmy pewne bariery, znów udowodniliśmy sobie, że można czegoś dokonać. Ale chciałbym Pana poprosić o odpowiedź na podstawowe pytanie: po co?

Naturalnie, kiedy pracujemy nad jakąś technologią, nasuwa się pytanie o sens inwestowania w nią pracy i środków. Po co nam kwantowa kryptografia? Odpowiedź, gdy porówna się świat sprzed dziesięciu lat z obecnym, nasuwa się sama: żeby chronić swoją prywatność.

A czym różni się kryptografia kwantowa od tradycyjnych metod?

Po pierwsze każda próba *podsłuchania* komunikacji zostanie wykryta, co wynika z praw mechaniki kwantowej – a więc nie możemy tego obejść. Po drugie, dysponując komputerami kwantowymi możemy stosunkowo łatwo złamać tradycyjne szyfry, jak popularny kiedyś RSA.

Pamięta Pan, jak dziesięć lat temu firma Quantum Network Solutions udostępniła dla swoich klientów możliwość nawiązania szyfrowanego kwantowo połączenia?

Pewnie, że pamiętam *(śmiech)*. Byłem bardzo szczęśliwy i nie mogłem się doczekać, kiedy z kolegami i koleżankami z instytutu wypróbujemy tą technologię. Jak pewnie większość z nas doskonale wie, rozgorzały wtedy liczne dyskusje, czy aby na pewno należy udostępniać taką usługę osobom prywatnym. Ja wierzyłem, że tak – jak widać miałem rację *(śmiech)*. Zresztą, już wtedy media uznały kryptografię kwantową za początek kwantowej rewolucji – bo przecież nie potrafiliśmy jeszcze wtedy dokonywać teleportacji bardziej złożonych obiektów, a komputer kwantowy też nie każdy miał w domu.

Mówi pan o licznych dyskusjach, towarzyszących początkom kryptografii kwantowej dla wszystkich. Czego dotyczyły i jaki jest pana pogląd na nie po tych wszystkich latach?

Z pewnością były słuszne... Tak jak zwykle były wynikiem swoistej obawy, czy nowa technologia jest już na tyle dojrzała, by móc ją udostępnić wszystkim chętnym. Ale poza aspektami technicznymi, poruszano w nich jeszcze jedną, niebywale ważną kwestię: czy społeczeństwo było gotowe na takie możliwości, jakie ze sobą niosła.

Obawiano się, że komunikacja, którą ciężko jest odszyfrować, a o każdej próbie takiego działania dowiedzą się natychmiast użytkownicy, będzie sprzyjać łamaniu prawa. Krótko mówiąc, bano się zagrożenia dla porządku publicznego ze strony różnych grup. Bo przecież nawet jeśli policja, czy służby specjalne, mogłyby w jakiś sposób podsłuchać plany takich ludzi, oni od razu by się o tym dowiedzieli i zmienili je, a do komunikacji użyli innego kanału.

Na szczęście okazało się, że kiedy śledzenie i podsłuchiwanie stają się niemożliwe, jedynym racjonalnym wyjściem jest zwiększenie starań o odpowiednią edukację społeczeństwa, o to, by ludzie szanowali się nawzajem. Zachowano ich prawo do prywatności.

Czyli jednym słowem, kiedy nie można było dla dobra ogółu poświęcić prawa do prywatności, jedyne możliwe wyjście wcale nie okazało się takie złe?

Tak, dokładnie. Możemy się zastanawiać, jak ważną wartością jest prywatność – czy nie warto poświęcić prywatności jakiejś grupy podejrzanych osób dla dobra większości. Ale rozumując w ten sposób dochodzimy do bardzo niebezpiecznych wniosków, bo może warto poświęcić i inne wartości?

Wydaje mi się, że możliwość przekazania komuś wiadomości tak, by nikt inny się o niej nie dowiedział jest swojego rodzaju naturalnym prawem każdej osoby. Pamiętajmy, że nie każdy podejrzany jest winny. Mój znajomy może przykładowo okradać banki, ale ja o tym nie wiem. Koresponduję z nim, czyli dla policji jestem także podejrzanym. Tymczasem jedyne, o czym rozmawiamy, to moje problemy rodzinne. Nie chciałbym, żeby ktoś to czytał (bo chociażby nie mam pojęcia jak ta informacja może zostać użyta) i mam prawo nikomu na to nie pozwalać. Podoba mi się, że obecnie podejście „tego ci nie wolno" zmienia się w „nie powinieneś, bo..." - czyli zasady regulujące nasze życie społeczne ulegają racjonalizacji.

To dobrze?

Dobrze, ponieważ jeśli człowiek coś zrozumie, to może się z tym zgodzić, a wtedy będzie tego przestrzegał.

A co z użytkownikami, których nie dotyczy podobna sytuacja? Chodzi mi o zwyczajnych Kowalskich, siedzących w domu i przeglądających internet.

Dzięki kryptografii kwantowej mają pewność, że nikt nie próbuje wykraść ich danych – nie chodzi tylko o dane osobowe, jak adres zamieszkania, ale również o to, co lubią, kupują, jedzą, noszą. Spersonalizowane reklamy są przez jednych chwalone (i nic dziwnego, same w sobie nie są niczym złym), ale drudzy podkreślają, że mogą prowadzić do manipulacji konsumentami. Znając czyjeś gusta, marketingowcy łatwo mogą zmusić daną osobę do zakupu. Chyba nie muszę mówić, jak lukratywny jest to rynek.

Panie profesorze, podsumowując – to dobrze, że każdy może dziś skorzystać z kryptografii kwantowej?

Tak. Cieszę się, że wpłynęła nie tylko na usługi sieciowe, ale i na nas samych oraz nasze społeczeństwa. Dziś możemy mieć pewność, że nasza prywatność jest dobrze chroniona.

Dziękuję za wywiad.

Źródło: *Technologie*, nr 8/2027.

Bibliografia:

- http://www.fuw.edu.pl/~szczytko/NT/materialy/9_QC/iqip.pdf
- http://www.fuw.edu.pl/~szczytko/NT/materialy/9_QC/grover.html
- http://obfusc.at/ed/cryptography_pl.html