Atak klonów: banki na kwantowym podsłuchu

Kwantowe systemy kryptograficzne - stosowane głównie przez rządy i banki - nie są tak bezpieczne jak dotychczas sądzono. W polsko-czeskich badaniach udowodniono, że nie trzeba łamać praw fizyki, by sklonować przesyłany kwantowo klucz kryptograficzny.

Wyniki badań opublikowano w kwietniu w "Physical Review Letters". W badaniach uczestniczył dr Karol Bartkiewicz z Uniwersytetu Palackiego w Ołomuńcu, prof. Adam Miranowicz z Uniwersytetu Adama Mickiewicza w Poznaniu, a także czescy badacze z jednostek badawczych w Ołomuńcu.

Chociaż do uzyskania sprawnych komputerów kwantowych jest jeszcze daleka droga, mechanikę kwantową wykorzystuje się już od wielu lat w szyfrowaniu. Kwantowe systemy kryptograficzne są stosowane głównie przez rządy i banki do transmisji poufnych danych. Klucz do odszyfrowania informacji przesyłany jest np. w wiązce odpowiednio spolaryzowanych fotonów. Prawa mechaniki kwantowej sprawiają, że nie można "podsłuchać" tak przesłanej informacji, nie będąc zauważonym - podsłuchiwanie powoduje wystąpienie w kluczu błędów.

"Dotychczas sądzono, że klucza nie da się podsłuchać, ale przy założeniu, że podczas jego przesyłania nie pojawiły się żadne błędy" - mówi kierownik badań, dr Karol Bartkiewicz. Wyjaśnia jednak, że założenie jest nierealistyczne - podczas kwantowego przesyłania danych zawsze pojawiają się jakieś zaburzenia, które mają związek np. z niedoskonałością światłowodów, którymi przesyłana jest informacja. Strony zazwyczaj akceptują pewien poziom błędów, które w tej komunikacji występują.

Tymczasem jak się okazuje, hakerzy mogą sklonować klucz szyfrujący i "schować" swoją aktywność w szumie - efekty klonowania klucza mogą być łatwe do pomylenia ze zwykłymi zakłóceniami, które zawsze pojawiają się podczas transmisji klucza.

Prace kierowane przez dr. Bartkiewicza pokazały, że bezpieczeństwo klucza jest zagrożone, kiedy poziom błędów przekroczy 18,5 proc. Jeśli więc okaże się, że w procesie ustalania klucza 1/5 informacji to szum, nie powinniśmy uznać klucza za bezpieczny - przy takim poziomie szumów strony powinny wziąć pod uwagę, że mogą być na podsłuchu. Tymczasem dotychczas taki poziom szumu mógł być jeszcze akceptowany.

"Do tej pory takie analizy bezpieczeństwa były przeprowadzane teoretycznie. My pokazaliśmy, że można zbudować fizyczny układ, który zbliża się do teoretycznej granicy bezpieczeństwa" - wyjaśnia badacz.

Na czym w uproszczeniu polega kryptografia kwantowa? Podczas procesu ustalania klucza kryptograficznego, jedna strona - Alicja - losuje klucz i wysyła ciąg fotonów o konkretnym stanie polaryzacji do drugiej osoby - Boba. Bob mierzy stan polaryzacji tych fotonów. Przypisuje tym stanom wartości 0 lub 1. Jawnie informuje Alicję, jak ustawił detektory, a Alicja wyjaśnia, gdzie się pomylił. W ten sposób kwantowo ustalany jest klucz binarny. Dzięki temu kluczowi można potem zaszyfrować tajną wiadomość i tak zakodowaną umieścić nawet w ogólnodostępnym miejscu. Bez klucza odszyfrowanie wiadomości jest praktycznie niemożliwe. Zgodnie z prawami fizyki nie można "podsłuchać" transmisji kwantowego klucza fotonów, nie wprowadzając do niego żadnych zmian.

W swojej pracy zespół dr. Bartkiewicza pokazał, że podsłuchiwacz - Ewa - może wykorzystać dodatkowy foton, o dokładnie poznanej polaryzacji. Ewa swoim fotonem może odbić foton będący bitem klucza. Chociaż foton z klucza podróżuje dalej od Alicji do Boba, to foton Ewy zostanie zmieniony podczas tego oddziaływania i Ewa może rozpoznać dane.

Zespół wykazał, że ślady pozostawiane przez podsłuchiwacza mogą być bardziej dyskretne niż dotąd sądzono. Jednak przy optymalnym klonowaniu klucza w ciągu bitów klucza powstawać musi co najmniej 18,5 proc. błędów. "Jeśli w kluczu mamy wyższy poziom błędów, powinniśmy zrezygnować z szyfrowania takim kluczem poufnej wiadomości" - uważa dr Bartkiewicz.

PAP Nauka w Polsce, Ludwika Tomala