Problemy kryptograficzne można złamać drogą wyżarzania kwantowego

9 listopada 2021

Czy kryptografia stosowana m.in. w bankach pozostanie bezpieczna, gdy do gry wejdą komputery kwantowe? Odpowiedzi na to pytanie pomogą udzielić badania dra inż. Michała Wrońskiego z Wojskowej Akademii Technicznej.

Wiele algorytmów kryptograficznych opiera się na problemie logarytmu dyskretnego na krzywych eliptycznych. Do tej pory nie udało się go złamać w praktyce (nawet dla bardzo małych przypadków) z wykorzystaniem metod kwantowych. Póki co, szyfry są bezpieczne.

„Bardzo dużo nam jeszcze brakuje, aby złamać logarytm dyskretny na krzywych eliptycznych dla przypadków wykorzystywanych w praktyce. Ale jeżeli to nastąpi, to współczesna kryptografia, chociażby ta, stosowana w bankach, będzie podatna na ataki, przede wszystkim z wykorzystaniem wariantów algorytmu Shora. Dlatego też prowadzi się obecnie intensywne badania nad algorytmami, które są odporne także na działanie komputerów kwantowych” – wyjaśnia sens swoich badań mjr dr inż. Michał Wroński.

Naukowiec z Instytutu Matematyki i Kryptologii podczas International Conference on Computational Science 2021 pokazał, jak można przekształcić znany atak na logarytm dyskretny na krzywych eliptycznych do postaci rozwiązywalnej przez komputery wykorzystujące wyżarzanie kwantowe (rodzaj obliczeń przynoszących bardzo szybkie rozwiązania).

Główny element tak zwanej metody indeksu, którym jest zbieranie zależności pomiędzy punktami krzywej eliptycznej, naukowiec przekształcił do problemu QUBO. Problem ten może być

następnie rozwiązywalny za pomocą wyżarzania kwantowego.

Do badań praktycznych dr inż. Wroński wykorzystał zdalny dostęp do komputera D-Wave. Udało mu się złamać problem logarytmu dyskretnego dla krzywej eliptycznej zadanej nad ciałem 8-bitowym.

Badacz przyznaje, że zrealizowany przykład nie jest duży, ale zaprezentowana przez niego metoda kwantowa dała rozwiązanie największego dotąd problemu logarytmu dyskretnego na krzywych eliptycznych.

„Badania przekształcania problemów kryptograficznych do problemów rozwiązywalnych z wykorzystaniem wyżarzania kwantowego powinny być w dalszym ciągu dynamicznie prowadzone, gdyż dzięki temu możliwy jest znaczny postęp w tej dziedzinie wiedzy" – podkreśla autor.

Artykuł źródłowy „Index Calculus Method for Solving Elliptic Curve Discrete Logarithm Problem Using Quantum Annealing" można przeczytać TUTAJ.

Autorstwo: Karolina Duszczyk
Źródło: NaukawPolsce.PAP.pl