Jerzy Klamka
Alina Otolińska
Wyższa Szkoła Biznesu

Wprowadzenie do kryptografii kwantowej

W klasycznej informatyce pojedynczy bit może przyjmować tylko dwie ustalone wartości logiczne, to znaczy 0 lub 1. Natomiast elementarną jednostką informatyki kwantowej jest kwantowy bit, w skrócie zwany qubitem, będący spinem atomu. Istotną cechą mechaniki kwantowej mającą zastosowanie w kryptografii kwantowej jest zjawisko splątania występujące między dwoma układami kwantowymi. Zjawisko to pozwala, by układy kwantowe wchodziły ze sobą we wzajemne związki, które w komputerze kwantowym odgrywają rolę kabla łączącego poszczególne qubity. Specjalnym przypadkiem splątania jest paradoks EPR (Einstein, Poldolsky i Rosen) mówiący, że tak długo jak stany kwantowe pozostają nieobserwowalne, ich własności pozostają niesprecyzowane, w superpozycji wszystkich stanów kwantowych. Zjawisko splątania jest efektem wykonania iloczynu tensorowego na 2-wymiarowych wektorach reprezentujących poszczególne qubity.

W pracy przedstawiono model matematyczny układu kwantowego złożonego z dwóch qubitów (kwantowych bitów). Następnie zdefiniowano pojęcie splątania w układach kwantowych na przykładzie układu kwantowego dwóch qubitów. Zjawisko splątania może być wykorzystane do bezpiecznego przesyłu informacji w sieciach kwantowych.

Należy również zaznaczyć, że w informatyce kwantowej występuje zjawisko utraty informacji zwanej dekoherencją. Dekoherencja oznacza zmianę własności qubitu, a więc również układu qubitów wraz z upływem czasu. Jest ono bezpośrednim efektem oddziaływania kwantowego układu z otoczeniem qubitów. Zjawisko o podobnym charakterze nie istnieje w klasycznej informatyce. Dekoherencja stanowi istotny, trudny do rozwiązania w praktyce problem techniczny. Występowanie zjawiska dekoherencji znacznie utrudnia przeprowadzanie poprawnej analizy matematycznej stanów kwantowych oraz ewentualną konstrukcję pojedynczych bramek kwantowych i układów bramek kwantowych.