ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2012
Seria: ORGANIZACJA I ZARZĄDZANIE z. 61 Nr kol. 1873

Marcin SOBOTA
Politechnika Śląska
Wydział Organizacji i Zarządzania
Instytut Ekonometrii i Informatyki

TEORIE KWANTOWE JAKO PODSTAWA NOWOCZESNEJ KRYPTOGRAFII

Streszczenie. Artykuł przedstawia kilka fundamentalnych praw oraz twierdzeń mechaniki kwantowej, stanowiących podstawę kryptografii kwantowej.

QUANTUM TEORIIES AS MODERN CRYPTOGRAPHY BASIS

Summary. This paper presents some fundamental rights and theorems of quantum mechanics stands base of quantum cryptography.

1. Wstęp

Mechaniką kwantową zaczęto się interesować w latach 20. XX wieku. Za ojców tej dziedziny nauki uważa się przede wszystkim Wernera Heisenberga[1] oraz Erwina Schrödingera[2]. Niemały wkład w jej rozwój wnieśli także Max Born[3], Paul Dirac[4], Niels Born[5], Richard Feynman[6] oraz Albert Einstein[7], mimo iż ten ostatni z interpretacją pewnych zjawisk nie pogodził się do końca życia i raczej jest kojarzony z fizyką dużych obiektów

[1] Werner Heisenberg sformułował zasadę nieoznaczoności.
[2] Erwin Schrödinger to twórca teorii mechaniki falowej.
[3] Max Born sformułował interpretację kwadratu funkcji falowej w równaniu Schrödingera jako gęstości prawdopodobieństwa znalezienia cząstki.
[4] Paul Dirac zunifikował mechanikę kwantową ze szczególną teorią względności oraz wprowadził notację stanów bra-ket.
[5] Niels Born wyjaśnił skwantowanie poziomów energetycznych w atomie wodoru oraz przyczynił się do stworzenie fizyki kwantów.
[6] Richard Feynman to twórca elektrodynamiki kwantowej.
[7] Albert Einstein wyjaśnił zjawisko fotoelektryczne.

(planety, gwiazdy). Pojawiające się nowe odkrycia oraz prowadzone doświadczenia niejednokrotnie dawały zadziwiające wyniki, pozostające w sprzeczności z mechaniką klasyczną.

Jedną z podstawowych cech świata kwantów jest czysta losowość zachodzących zjawisk, pozwalająca jedynie na określenie prawdopodobieństwa danego zajścia. Mówiąc inaczej, nie da się przewidzieć np. zachowania pojedynczej cząstki, a jedynie można określić prawdopodobieństwo takiego czy innego zachowania. Jeśli skierujemy strumień fotonów w kierunku szyby, to możemy określić, że 95% fotonów przejdzie przez szybę, natomiast 5% fotonów odbije się od niej. Nie jesteśmy jednak w stanie przewidzieć zachowania pojedynczego fotonu (nie jesteśmy w stanie określić, czy foton przejdzie przez szybę, czy się od niej odbije). I nie wynika to z braku naszej wiedzy bądź niedoskonałości sprzętu, ale z natury świata kwantów.

2. Prawa mechaniki kwantowej a kryptografia

Prawa mechaniki kwantowej leżą u podstaw niemal całej współczesnej nauki i techniki. Wykorzystuje się je w realizacji tranzystorów i układów scalonych. Stanowią również podstawę takich dziedzin nauki, jak biologia czy chemia. Spośród nauk fizycznych jedynie kosmologia i grawitacja nie zostały w pełnym stopniu uzgodnione z mechaniką kwantową. W dalszej części zostaną przedstawione zasady mechaniki kwantowej, dzięki którym można wykorzystać ją w kryptografii.

2.1. Spin

Spin to moment własny pędu cząstki w układzie, w którym nie wykonuje ona ruchu postępowego. Własny oznacza tu taki, który nie wynika z ruchu danej cząstki względem innych cząstek, lecz tylko z samej natury tej cząstki. Każdy rodzaj cząstek elementarnych ma odpowiedni dla siebie spin. Jest on wielkością kwantową, która nie ma klasycznego odpowiednika. Spin często jest przedstawiany jako rotacja wirującego bąka, choć taka prezentacja jest myląca ze względu na to, że zgodnie z mechaniką kwantową cząstki nie mają żadnej dobrze określonej osi. Wydaje się, że lepsze jest powiedzenie, iż spin to wewnętrzna właściwość cząstki elementarnej, określająca jak wygląda ta cząstka z każdej strony. We wszechświecie występują cząstki o spinach całościowych i połówkowych. Cząstki o spinach połówkowych są nazywane fermionami i stanowią budulec materii we wszechświecie. Można do nich zaliczyć elektrony, miony czy neutrina. Cząstki o spinie całkowitym są nazywane bozonami i są to cząstki przenoszące oddziaływania. Można do nich zaliczyć grawitony oraz fotony. Jeśli cząstka ma spin równy 1, oznacza to, że należy obrócić ją

o 360^0, żeby wyglądała tak jak przed obrotem. Jeśli cząstka ma spin równy 2, to trzeba ją obrócić o kąt równy 180^0 i tak dalej. W przypadku cząstek o spinie połówkowym kąt obrotu jest większy niż 360^0. Jeżeli mamy do czynienia z cząstką o spinie równym ½, to pierwotny wygląd uzyskamy po obróceniu cząstki o 720^0. Co nam daje spin z punktu widzenia kryptografii? Spin ma własność, dzięki której jesteśmy w stanie zakodować wartości zero-jedynkowe. Jeśli wyobrazimy sobie foton, który jest cząstką o spinie równym 1, to poszczególne polaryzacje fotonu mogą nam reprezentować wartości 0 i 1. Za pomocą tych polaryzacji można kodować odpowiednie wartości, a dokonując odczytu polaryzacji, możemy się dowiedzieć, czy reprezentował on stan 0 czy 1. Mówiąc inaczej, odpowiednikiem klasycznego kodowania (0 to stan niski, 1 to stan wysoki) jest ustawienie odpowiedniej polaryzacji fotonu.

2.2. Zasada nieoznaczoności Heisenberga

Zasada nieoznaczoności Heisenberga mówi, że istnieją takie pary wielkości, których nie da się jednocześnie zmierzyć z dowolną dokładnością. Są to wielkości, które nie komutują. Akt pomiaru jednej wielkości wpływa na układ w taki sposób, że tracona jest część informacji o drugiej wielkości. Zasada nieoznaczoności wynika z natury rzeczywistości i nie ma nic wspólnego z niedoskonałością metod ani instrumentów pomiaru. Matematycznie zasada nieoznaczoności przedstawiona jest następująco:

$$\Delta x \Delta p \geq \frac{h}{4\pi}, \tag{1}$$

gdzie:

Δx – nieokreśloność pomiaru położenia,

Δp – nieokreśloność momentu pędu,

h – stała Plancka,

co należy interpretować w ten sposób, że jeżeli zwiększamy dokładność pomiaru jednej wartości, zmniejsza się dokładność pomiaru drugiej. Pełna informacja na temat położenia cząstki oznacza brak jakiejkolwiek informacji na temat jej momentu pędu. Zasada nieoznaczoności ma fundamentalny wpływ na budowę znanego nam świata. Tłumaczy między innymi, dlaczego w atomie występują powłoki i dlaczego występują one w takich, a nie innych odległościach od jądra.

Zasada nieoznaczoności Heisenberga ma decydujące znaczenie w kwantowych protokołach uzgadniania klucza szyfrującego. Rozpatrzymy przypadek protokołu BB84 [1]. Twórcami protokołu są: Charles Bennett i Gilles Brassard. Opiera się on na zastosowaniu dwóch alfabetów:

- prostego, zawierającego fotony o polaryzacji 0^0 i 90^0 (binarne 0 i 1),
- ukośnego, zawierającego fotony o polaryzacji 45^0 i 135^0 (binarne 0 i 1).

Rys. 1. Alfabety wykorzystane w protokole BB84
Fig. 1. Alphabets used in BB84 protocol

Zgodnie z zasadą nieoznaczoności Heisenberga niemożliwe jest dokonanie pomiaru jednocześnie w bazach prostej i ukośnej. Jeżeli odbiorca wiadomości dokona prawidłowego wyboru, tzn. wybierze pomiar w bazie prostej dla fotonu, którego polaryzacja należy do alfabetu prostego, to otrzyma prawidłowy wynik pomiaru (zarejestruje taką polaryzację fotonu, jaką faktycznie foton miał). Jeżeli jednak dobór bazy będzie nieprawidłowy, tzn. wybierze bazę ukośną dla polaryzacji z alfabetu prostego, to z prawdopodobieństwem równym ½ otrzyma w wyniku pomiaru jedną z polaryzacji należących do alfabetu ukośnego. W tym przypadku nieoznaczoność wymusza konieczność dokonania wyboru jednej z dwóch możliwych baz, a to z kolei prowadzi do uzyskania prawidłowego lub nieprawidłowego wyniku.

Zasada nieoznaczoności uniemożliwia uniknięcie błędnych pomiarów (dokonanie pomiarów zawsze wprowadza zmiany polaryzacji fotonów nadawcy), a to z kolei powoduje, że każda próba podsłuchu na drodze nadawca-odbiorca może zostać wykryta. Innymi słowy, każdy akt pomiaru jest aktywny (nie da się „przyjrzeć" układowi z boku), a skoro tak, to dzięki zasadzie nieoznaczoności aktywność ta może zostać wykryta. Dodatkowo zasada nieoznaczoności jest wspierana tzw. twierdzeniem o niekłonowaniu. Z twierdzenia wynika, że nie istnieje transformacja unitarna U taka, że $U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$ dla dowolnego stanu kwantowego $|\Psi\rangle$. Jeśli by przyjąć, że istnieje takie U, że $U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$ oraz $U|\Phi\rangle|0\rangle = |\Phi\rangle|\Phi\rangle$ dla dowolnych $|\Psi\rangle$ i $|\Phi\rangle$, to transformacja U reprezentowałaby maszynę klonującą. Z unitarności macierzy U wynika jednak, że $\langle\Psi|\langle 0|U^{+}U|\Phi\rangle|0\rangle = \langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle$ oraz $\langle\Psi|\Phi\rangle\langle 0|0\rangle = \langle\Psi|\Phi\rangle\langle\Psi|\Phi\rangle$, co nie jest prawdziwe dla dowolnych stanów kwantowych $|\Psi\rangle$ i $|\Phi\rangle$, może natomiast zachodzić dla stanów ortogonalnych $\langle\Psi|\Phi\rangle = \{0, 1\}$. Oznacza to,

że nie da się sklonować nieznanego stanu kwantowego celem dokonania na nim wielokrotnych pomiarów, prowadzących do uzyskania prawidłowego wyniku z ominięciem zasady nieoznaczoności.

2.3. Twierdzenie Bella i splątanie

Splątanie jest efektem wykonania iloczynu tensorowego na 2-wymiarowych wektorach, reprezentujących poszczególne qubity. Z własności iloczynu tensorowego wynika, że na podstawie wektora będącego wynikiem wykonania iloczynu tensorowego nie można (poza szczególnymi przypadkami) określić wektorów będących czynnikami tego iloczynu. Oznacza to, że ogólnie przypadku stanu kwantowego $|\Psi\rangle \in \mathrm{H}^{2^n}$ nie można jednoznacznie przedstawić jako iloczynu tensorowego n stanów kwantowych $|\Psi_i\rangle \in \mathrm{H}^2$, $i = 1,2,3,...,n$, a skoro tak, tzn. że muszą występować wzajemne korelacje między stanami kwantowymi $|\Psi_i\rangle$. Niech: $|\Psi\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle) \in H^4$; wektor taki przedstawia splątany stan kwantowy, gdyż nie można znaleźć dwóch stanów kwantowych $|\Psi_1\rangle \in \mathrm{H}^2$ oraz $|\Psi_2\rangle \in H^2$, takich że $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$. Pojęcie splątania jest związane z tzw. bazą ortogonalną Bella, reprezentowaną w zespolonej przestrzeni Hilberta H^4 przez cztery, wzajemnie ortogonalne wektory bazowe:

$$|00\rangle + |11\rangle \in H^4,\ |00\rangle - |11\rangle \in H^4,\ |01\rangle + |10\rangle \in H^4,\ |01\rangle - |10\rangle \in H^4.$$

Dowolny układ kwantowy, składający się z 2 qubitów, jest splątany przez pewną 4x4-wymiarową macierz unitarną. Splątanie wykazuje niezależność od odległości, w jakiej znajdują się splątane fotony. Ta niezależność od odległości sugerowałaby, że sygnał informujący cząstki o tym, jak mają się zachować, porusza się szybciej niż światło w próżni. Z tym nie mógł się pogodzić Einstein, twierdząc, że muszą istnieć jakieś zmienne ukryte, zapisywane w momencie dokonywania splątania i mówiące cząstce, jak ma się zachować w momencie dokonania pomiaru. Teorię tę obalił Bell, dokonując wielu eksperymentów podsumowanych jednym z fundamentalnych twierdzeń w mechanice kwantowej, zwanym twierdzeniem Bella[1].

Splątanie znalazło zastosowanie w protokole E91 [3]. Źródło splątanych fotonów może być w posiadaniu jednej ze stron lub niezależne. Po wytworzeniu dwóch splątanych fotonów każda ze stron otrzymuje po jednym z nich. Dokonanie pomiaru na dowolnym fotonie powoduje zniszczenie stanu splątania, ale jednocześnie informuje, jakiej polaryzacji jest

[1] Żadna teoria zmiennych ukrytych zgodna z teorią względności nie może opisać wszystkich zjawisk mechaniki kwantowej.

drugi foton. Jeśli dokonany pomiar wskazał, iż mierzony foton ma polaryzację poziomą, to oznacza, że drugi foton w tym samym momencie przyjął polaryzację pionową.

3. Wnioski

W artykule przedstawiono następujące zasady i teorie kwantowe:

- Zasada nieoznaczoności Heisenberga.
- Twierdzenie o nieklonowaniu.
- Niemożność wykonania pasywnego podsłuchu.
- Splątanie.

Wszystkie wspomniane prawa, zasady i teorie zostały wykorzystane w opracowanych kwantowych protokołach uzgadniania klucza szyfrującego, takich jak: BB84, B92, E91, EPR czy SARG. Zasada nieoznaczoności Heisenberga wpływa na pojawianie się błędów pomiarowych, co pozwala na wykrycie ewentualnych intruzów podsłuchujących komunikację. Dodatkowo twierdzenie o nieklonowaniu oraz brak możliwości realizacji pasywnego podsłuchu uniemożliwiają ominięcie zasady nieoznaczoności. Odkrycie istnienia stanów splątanych pozwoliło na opracowanie protokołu pozwalającego na wykorzystanie tego zjawiska do uzgodnienia klucza.

Bibliografia

1. Bennett C.H., Brassard G.: Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing. Bangalore, India 1984.
2. Bennet C.H.: Quantum cryptography using any two non-orthogonal states. Physical Review Letters, Vol. 68, May 1992, pp. 3121-3124.
3. Bell J.S.: On the Einstein Podolosky Rosen Paradox. Physics, 1, 195-200, 1964, reprinted in Quantum Theory and Measurement, 1987, p. 403.
4. Ekert A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67, 1991, pp. 661-663.
5. Sobota M.: Wykorzystanie zjawiska splątania cząstek do przeprowadzenia teleportacji. Wysokowydajne sieci komputerowe. Nowe technologie. Wydawnictwa Komunikacji i Łączności, Warszawa 2005.

6. Sobota M.: Bezpieczeństwo wymiany klucza szyfrującego z wykorzystaniem wybranych protokołów kwantowych. Nowe technologie w komputerowych systemach zarządzania. Wydawnictwa Komunikacji i Łączności, Warszawa 2005.

Abstract

The article presents the following quantum principles and theories:

- Heisenberg uncertainty principle.
- Non-cloning theorem.
- Inability to comply with the passive eavesdropping.
- Entanglement.

All mentioned rights, principles and theories have been used in quantum cryptographic key agreement protocols such as BB84, B92, E91, EPR or SARG. Heisenberg uncertainty principle effects the occurrence of errors of measurement which allows to detect potential intruders Privacy Snoops communication. Additionally non-clioning theorem and the lack of feasibility of passive eavesdropping impossible to circumvent the uncertainty principle. Discovery of the existence of entangled states allowed to develop a protocol that enables the use of this phenomenon to agree on the key.