Roman GIELERAK, Marek SAWERWAIN, Przemysław RATAJCZAK
UNIWERSYTET ZIELONOGÓRSKI, INSTYTUT STEROWANIA I SYSTEMÓW INFORMATYCZNYCH

Probabilistyczny protokół transferu klasycznej informacji w kanale kwantowym

prof. dr hab. Roman GIELERAK

Wszystkie stopnie i tytuły naukowe uzyskał na Uniwersytecie Wrocławskim w okresie od 1976 do 1999(profesura). Brał udział w licznych projektach badawczych we współpracy z wieloma ośrodkami zagranicznymi (ETH Zurych; ZIBJ Dubna; MGU Moskwa; Bochum-Bonn-Bielefeld Uniwersytety; Instytut Galileusza, Paryż; Uniwersytet w Lisbonie). Autor licznych prac i opracowań monograficznych z podstaw teorii kwantowej i jej zastosowań.

e-mail: R.Gielerak@issi.uz.zgora.pl

mgr inż. Przemysław RATAJCZAK

Ukończył studia na Wydziale Elektrotechniki, Informatyki i Telekomunikacji Uniwersytetu Zielonogórskiego. W roku 2006 obronił pracę magisterską pt. Protokoły kryptografii kwantowej i ich symulacje komputerowe. Aktualnie pracuje jako asystentem na Wydziale Elektrotechniki, Informatyki i Telekomunikacji UZ.

e-mail: P.Ratajczak@issi.uz.zgora.pl

mgr inż. Marek SAWERWAIN

Ukończył studia na Wydziale Elektrotechniki, Informatyki i Telekomunikacji Uniwersytetu Zielonogórskiego. Aktualnie pracuje jako asystent w Instytucie Sterowania i Systemów Informatycznych. Zajmuje się kwantowymi językami programowania, oraz operacyjną semantyką dla procesów kwantowych. Pracuje również nad symulatorem kwantowego modelu obliczeniowego dla systemów jedno oraz wieloprocesorowych oraz wersji sieciowej.

e-mail: M.Sawerwain@issi.uz.zgora.pl

Streszczenie

W oparciu o znane protokoły teleportacji czystych stanów kwantowych dokonano analizy możliwości transferu klasycznej informacji w kanale kwantowym. Potencjalną przewagą omawianego protokołu byłby brak konieczności dodatkowej transmisji klasycznej informacji do korekcji teleportowanych stanów. Bowiem, w miejsce dodatkowego transferu w kanale klasycznym, który jest niezbędny w przypadku znanych protokołów teleportacji, zaproponowano dwa mechanizmy prowadzące do możliwości statystycznego odróżniania dwóch ortogonalnych stanów kwantowych. Pierwszy mechanizm, to reguła odpowiedniego osłabiania maksymalnego splątania w początkowej fazie teleportacji, natomiast drugim równoważnym mechanizmem jest pomiar pary splatanej utworzonej przez stan teleportowany w bazach niekanonicznych.. Jako pierwsze zastosowanie opisano nowy protokół transferu klucza klasycznego w kanale kwantowym przy implementacji protokołu Vernama, a także rozpoczęto dyskusję aspektów bezpieczeństwa proponowanego protokołu.

Abstract

In this paper we give proposition of new classical information transfer scheme. It is based on qubit teleportation scheme, but there is no need to send additional information via classical channel. This assumption allows as to consider probabilistic protocol of data transfer. In particular, we analyze the case where the statistical methods are used to distinguish orthogonal quantum states. We describe two methods used for this process. The first is changing the maximally entangled state to the non-maximally one that leads to a teleported state with reduced fidelity and the second is measurement of teleported state in non-canonical bases.

Słowa kluczowe: protokół kwantowej teleportacji probabilistycznej, kryptografia kwantowa

Keywords: quantum probabilistic teleportation, quantum cryptography

1. Wstęp: teleportacje stanów kwantowych

Niech Σ_1 i Σ_2 będą dwoma układami fizycznymi zlokalizowanymi w obszarach Θ_1, odp. Θ_2 czasoprzestrzeni, którą modelujemy za pomocą czasoprzestrzeni Minkowskiego o sygnaturze 3. Z fundamentalnych praw fizyki wynika, że możliwość komunikowania się układu Σ_1 z układem Σ_2 jest możliwa wtedy i tylko wtedy, gdy powłoki kauzalne obszarów Θ_1 i Θ_2 mają niepuste przecięcie.

Zasada ta znana jest pod nazwą lokalności świata rzeczywistego i z pewną dozą nadinterpretacji uwypukla ona paradygmat fizyki mówiący, że istnieje górne ograniczenie na transfer informacji klasycznej: nie można transmitować informacji w kanałach klasycznych szybciej, niż z prędkością światła w próżni $c \cong 3*10^6$ km/s.

Zupełnie inaczej wygląda ta kwestia w kanałach kwantowych. Jeżeli teraz układy Σ_1 i Σ_2 są układami kwantowymi, które znajdują się w splątanym stanie kwantowym $\Psi_{\Sigma_1 \cap \Sigma_2}$, to może się zdarzyć, że lokalne operacje wykonywane na układzie Σ_1 znajdują swój wyraz w natychmiastowej zmianie stanu w jakim znajduje się podukład Σ_2 (z punktu widzenia obserwatora układu Σ_2). Zjawisko to znane jest pod nazwą nielokalności świata na poziomie kwantowym, a geneza jego sięga pracy [1], zaś różne, czasami zaskakujące konsekwencje tego zjawiska są intensywnie dyskutowane na różnych poziomach do dzisiaj i ciągle wydają się nie w pełni zrozumiałe [2]. Ewentualna nielokalność świata na poziomie kwantowym jest weryfikowalna w sposób eksperymentalny [3, 4, 5] poprzez weryfikacje tzw. statystycznych nierówności Bella a wieloletni postęp tego eksperymentu coraz bardziej nas przybliża do konkluzji, iż na poziomie kwantowym świat jest nielokalny.

Jednym z najbardziej spektakularnych osiągnięć informatyki kwantowej w ostatnich latach było odkrycie protokołów teleportacji stanów kwantowych [6] przez użycie kanałów kwantowych implementowanych poprzez układy kwantowe o maksymalnym poziomie splątania. Zilustrujemy podstawowe idee standardowego protokołu teleportacji opisem możliwych scenariuszy procesu teleportacji czystych stanów układu jednokubitowego; warto tutaj podkreślić istnienie teoretycznych algorytmów do teleportacji dowolnych stanów nawet bardzo złożonych układów kwantowych [7] oraz systematycznie dokonujący się postęp w implementacjach laboratoryjnych procesu teleportowania stanów kwantowych [8,9]. Opiszemy teraz standardowy deterministyczny algorytm teleportowania czystych stanów jednoqubitowych [10].

Załóżmy, że układ jednokubitowy indeksowany przez Θ znajduje się w stanie $|\psi\rangle_0 = \alpha |0\rangle_0 + \beta |1\rangle_0$, gdzie $\alpha, \beta \in C$, $|\alpha|^2 + |\beta|^2 = 1$, a $|0\rangle_0, |1\rangle_0$ to kanoniczna baza ortonormalna przestrzeni stanów C^2. Zakładamy także, że nadawca i potencjalny odbiorca dzielą wspólny układ dwuqubitowy indeksowany przez 1 i 2 znajdujący się w stanie:

$$|\Theta_0\rangle_{1,2} = \alpha_{00} |00\rangle_{12} + \alpha_{01} |01\rangle_{12} + \alpha_{10} |10\rangle_{12} + \alpha_{11} |11\rangle_{12}, \quad (1.1)$$

gdzie $\alpha_{ij} \in C, |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$,

przy czym dodatkowo zakładamy, że qubit indeksowany liczbą 1 jest do dyspozycji nadawcy. Standardowy algorytm teleportowania stanów $|\Psi\rangle_0$ do odbiorcy $|\bullet\rangle_2$ przebiega wedle schematu:

T1. Przygotowujemy $|\Theta\rangle_{1,2}$ jako maksymalnie splątany stan Bella: $|B\rangle_{1,2} = \frac{1}{\sqrt{2}}(|00\rangle_{1,2} + |11\rangle_{1,2})$ (1.2)

T2. Biorąc pod uwagę tożsamość:

$$(CNOT \otimes I)(H \otimes I \otimes I)|\psi\rangle_0 |B\rangle_{1,2} = |00\rangle_{0,1}|\psi\rangle_2 + |10\rangle_{0,1} i\sigma_y |\psi\rangle_2 + |01\rangle_{0,1}\sigma_x|\psi\rangle_2 + |11\rangle_{0,1}\sigma_x i\sigma_y |\psi\rangle_2 \quad (1.3)$$

i wykonując pomiar w bazie kanonicznej $|ij\rangle_{0,1}$ na qubitach 0 i 1 widzimy, że qubit indeksowany cyfrą 2 znajduje się w stanie: $|\psi\rangle_2$ gdy pomiar da wynik $|00\rangle_{0,1}$, $i\sigma_y|\psi\rangle_2$ gdy pomiar da wynik $|10\rangle_{0,1}$, $\sigma_x|\psi\rangle_2$ gdy pomiar da wynik $|01\rangle_{0,1}$ oraz w stanie $\sigma_z i\sigma_y|\psi\rangle_2$ gdy wynik pomiaru będzie równy $|11\rangle_{0,1}$.

T3. Nadawca przesyła w klasycznym kanale dwa bity klasyczne z wynikiem przeprowadzonego pomiaru, a wtedy odbiorca wykonuje operację korekcji stanu odpowiednią do jednej z operacji $\sigma_x, \sigma_y, \sigma_z$ na swoim qubicie.

Naszym celem jest próba skonstruowania takiej modyfikacji tego algorytmu, ażeby możliwe było teleportowanie wyróżnionych dwóch stanów, załóżmy $|0\rangle_0, |1\rangle_0$ w taki sposób, aby odbiorca poprzez przeprowadzenie elementarnej analizy statystycznej pomiarów stanów swojego qubitu był w stanie odpowiedzieć na pytanie co jest teleportowane do niego w serii repetycji. Jeżeli taki algorytm jest możliwy, to otworzy on drogę do teleportowania klasycznej informacji w kanale kwantowym bez ograniczeń typu ograniczenie prędkości światła. Jak wiemy jest to problem w komunikacji np. satelitarnej. Wystarczy przypomnieć, że sygnał radiowy (a więc komunikacji w kanale klasycznym) na Marsa biegnie około 15 minut, co uniemożliwia jakiekolwiek racjonalne sterowanie urządzeniami wysłanymi tam w wersji „in-time".
Jak widać, powyżej opisany deterministyczny algorytm teleportacji nie spełnia naszych wymagań, jako że, każda z czterech możliwości dotycząca stanu finalnego zachodzi z jednakowym prawdopodobieństwem równym ¼ i to dla każdego stanu wejściowego. Podstawowe modyfikacje standardowego algorytmu teleportacji rozważane przez nas dotyczą następujących kwestii:

M1. Osłabienie początkowego splątania.

Korzystając z rozkładu Schmidta wiemy, że dowolny stan dwukubitowy $|\Theta\rangle$ można przedstawić jednoznacznie w postaci:

$$\Theta = \sum \lambda_i |\Theta_i\rangle_1 |\Theta'_i\rangle_2 \quad (1.4)$$

gdzie ilość składników w sumie (1.4) odpowiada tzw. rankowi Schmidta, a współczynniki λ_i to tzw. liczby Schmidta wektora $|\Theta\rangle$. Im większy rank Schmidta, tym wyższy poziom splątania, a przy równym ranku decydują wartości liczb λ_i, a dokładniej ich uporządkowanie względem porządku leksygraficznego. Właśnie stany Bella to układ ortonormalny złożony z maksymalnie splątanych wektorów. Zatem jako najogólniejszy stan początkowy weźmiemy wektor postaci

$$|\Theta_1\rangle_2 = \lambda_1 |\Theta_1\rangle_1 |\Theta'_1\rangle_1 + \lambda_2 |\Theta_2\rangle_1 |\Theta'_2\rangle_2 \quad (1.5)$$

gdzie λ_1, λ_2 są takie, że $|\lambda_1|^2 + |\lambda_2|^2 = 1$, a $|\Theta_j\rangle_i$, odp $|\Theta'_i\rangle_i$, $i = 1,2$, $j = 1,2$ tworzą układy ortonormalne w C^4.

M2. Pomiar dowolnej obserwabli.

Zamiast robić standardowy pomiar jak w T2 postulujemy wykonanie pomiaru dla odpowiednio dobranej obserwabli A.

Niech $A = a_i E_1 + a_2 E_2 + a_3 E_3 + a_4 E_4$ (1.6)

będzie rozkładem spektralnym macierzy A. Wtedy mierząc wartość obserwabli A na naszym układzie w stanie $|\Psi\rangle_0 |\Theta\rangle_{12}$ otrzymujemy wartości a_i z prawdopodobieństwami odpowiednio $p_i = \left|{}_2\langle 0|\ {}_{0,1}\langle A_i | \Psi\rangle_0 |\Theta\rangle_{12}\right|^2 + \left|{}_2\langle 1|\ {}_{0,1}\langle A_i | \Psi\rangle_0 |\Theta\rangle_{12}\right|^2$, (1.7)

gdzie $|A_i\rangle$ to wektory własne A, tzn. $E_i = |A_i\rangle\langle A_i|$, a cały układ złożony z trzech qubitów znajdzie się w stanie

$$\frac{(F_i \otimes \mathrm{I})|\Psi\rangle_0 |\Theta\rangle_{12}}{\left\|(F_i \otimes \mathrm{I})|\Psi\rangle_0 |\Theta\rangle_{12}\right\|} \quad (1.8)$$

z prawdopodobieństwem równym (1.7).

M3. Pomiar obserwabli B.

Niech B będzie obserwablą mierzoną przez odbiorcę o numerze 2. Jeżeli układ po wykonaniu kroku M2 skolapsował do stanu (1.8) to wynik pomiaru obserwabli $B = b_1 G_1 + b_2 G_2$, gdzie $G_i = |G_i\rangle\langle G_i|$ to wektory własne B, a b_i to wartości własne, będzie równy b_i z prawdopodobieństwem

$$q_i = \frac{|{}_2\langle G_i | (F_i \otimes \mathrm{I})|\Psi\rangle_0 |\Theta\rangle_{12}|^2}{\left\|(F_i \otimes \mathrm{I})|\Psi\rangle_0 |\Theta\rangle_{12}\right\|^2} \quad (1.9)$$

gdzie $i = 1,2$, a qubit odbiorcy będzie po pomiarze B_2 w stanie $|G_i\rangle$.

Podstawowe pytanie jakie nas interesuje to :

Czy istnieje taka modyfikacja M1-M3 oryginalnego protokołu T1-T3 umożliwiająca statystyczne odróżnienie co najmniej dwóch stanów wejściowych np. $|0\rangle_0, |1\rangle_0$. Przez statystyczne rozróżnienie rozumiemy możliwość wykonania serii transmisji, a w rezultacie serii pomiarów B, w wyniku których prawdopodobieństwo pomiaru np. b_1 będzie zależeć od tego co podano na wejściu. Taki protokół będziemy nazywać probabilistycznym protokołem teleportacji klasycznej informacji.

Poniżej przedstawimy pewną wstępną wersję tego rodzaju modyfikacji algorytmu T1-T3 dającą nadzieję na jego realizację techniczną.

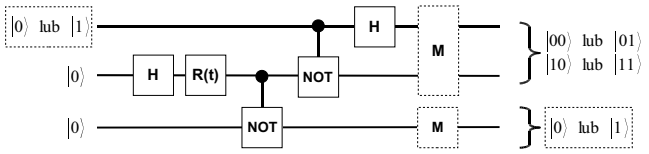
2. Algorytm statystycznej teleportacji klasycznej informacji

Deterministyczne algorytmy teleportacji stanu kwantowego wymagają przesyłania dodatkowej informacji celem korekcji teleportowanego stanu. Pominięcie tego kroku powoduje wprowadzenie błędu do teleportowanego stanu. W oryginalnym protokole (protokół teleportacji doczekał się także wielu realizacji eksperymentalnych [11]), tylko w jednym przypadku otrzymuje się stan oryginalny, natomiast w pozostałych trzech należy wykonać dodatkowe operacje, aby otrzymać oryginalny -- teleportowany -- stan. Oznacza to, iż prawdopodobieństwo otrzymania prawidłowego stanu wynosi ¼. Wartość tą można znacząco poprawić, jeśli zostanie ograniczona liczba możliwych stanów, jakie będą przesyłane. Idea teleportacji probabilistycznej jest dyskutowana w wielu pracach np.: [12], [13].

Podejście zaprezentowane na Rys. 1 przedstawia obwód kwantowy przeznaczony do teleportacji stanów zero oraz jeden z bardzo wysoką skutecznością. Zasadniczą różnicą względem oryginalnego protokołu jest pominięcie dodatkowych operacji korekcji stanu kwantowego. Istotna zmiana pojawia się także w pierwszym etapie, czyli podczas przygotowania odpowiednio zmienionego stanu splątanego. Stosowana jest dodatkowa bramka obrotu rzeczywistego o następującej postaci macierzowej:

$$R(\Theta)=\begin{bmatrix}\cos\Theta & -\sin\Theta\\ \sin\Theta & \cos\Theta\end{bmatrix} \qquad (2.1)$$

Następnie (w tym miejscu postępujemy identycznie jak w oryginalnym protokole teleportacji), należy wykonać dwie operacje unitarne, operację kontrolowanej negacji oraz operację Hadamarda. Kolejny krok, to wykonanie pomiaru na pierwszych dwóch qubitach. Jednakże, wyniki pomiaru, nie są przekazywane do drugiego uczestnika teleportacji. Stan zero bądź jeden, zostaje teleportowany do qubitu o numerze trzy. Oznacza to, iż należy wyznaczyć wartości prawdopodobieństwa oraz wykazać ich zależność od głównego parametru obwodu, jakim w przypadku obwodu z Rys. X1 jest bramka obrotu rzeczywistego o kąt theta.



Rys. X1: Obwód kwantowy teleportujący stan klasyczne zero bądź stan jeden
Fig. X1.: Quantum circuit to the teleportation of classical zero and one states

Przez ST_0 oraz ST_1 oznaczamy stan obwodu podczas teleportacji stanu zero oraz jeden. Przed wykonaniem operacji pomiaru na qubitach zero oraz jeden obydwa stany przyjmują następującą postać:

$$ST_0=\begin{bmatrix}0.5\cos\Theta-0.5\sin\Theta & (000)_2\\ 0 & (001)_2\\ 0 & (010)_2\\ 0.5\cos\Theta+0.5\sin\Theta & (011)_2\\ 0.5\cos\Theta-0.5\sin\Theta & (100)_2\\ 0 & (101)_2\\ 0 & (110)_2\\ 0.5\cos\Theta+0.5\sin\Theta & (111)_2\end{bmatrix},\quad ST_1=\begin{bmatrix}0 & (000)_2\\ 0.5\cos\Theta-0.5\sin\Theta & (001)_2\\ 0.5\cos\Theta+0.5\sin\Theta & (010)_2\\ 0 & (011)_2\\ 0 & (100)_2\\ -0.5\cos\Theta+0.5\sin\Theta & (101)_2\\ -0.5\cos\Theta-0.5\sin\Theta & (110)_2\\ 0 & (111)_2\end{bmatrix} \qquad (2.2)$$

Prawdopodobieństwo zmierzenia stanu podczas teleportacji zera, który będzie sprzyjał teleportacji stanu zero oraz stanu jeden jest równe odpowiednio:

$$P^0_{ST_0}(\Theta)=2\left|0.5\cos\Theta-0.5\sin\Theta\right|^2 \qquad (2.3)$$
$$P^1_{ST_0}(\Theta)=2\left|0.5\cos\Theta+0.5\sin\Theta\right|^2$$

Natomiast, w przypadku teleportacji stanu jeden, odpowiednio dla zera i jedynki otrzymamy

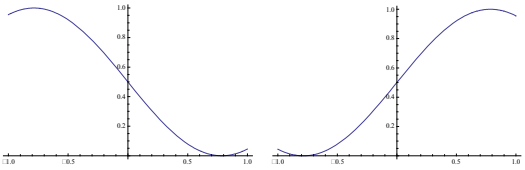
$$P^0_{ST_1}(\Theta)=\left|0.5\cos\Theta+0.5\sin\Theta\right|^2+\left|-0.5\cos\Theta-0.5\sin\Theta\right|^2 \qquad (2.4)$$
$$P^1_{ST_1}(\Theta)=\left|0.5\cos\Theta-0.5\sin\Theta\right|^2+\left|-0.5\cos\Theta+0.5\sin\Theta\right|^2$$

Ponieważ, uzyskane równania zależą od parametru theta, to również wielkość prawdopodobieństwa otrzymania zera bądź jedności zależą od wartości tego parametru.

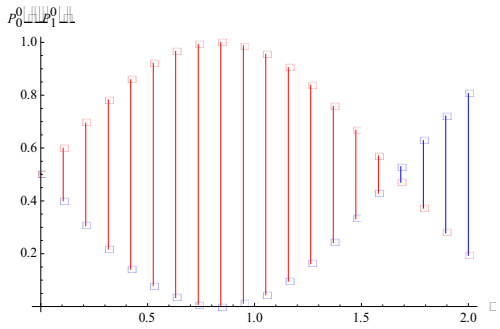
Rys. X2 przedstawia wykres wartości funkcji $P^0_{ST_0}(\Theta)$ oraz $P^1_{ST_0}(\Theta)$. Obydwie funkcje są okresowe, przy czym są przesunięte wzajemnie o wartość $\pi/2$, co oznacza, że minimum jednej z funkcji przypada na maksimum drugiej funkcji. W zależności od doboru parametru theta, można maksymalizować pomiar jednej z wartości. Chcąc zwiększyć prawdopodobieństwo otrzymania stanu zero podczas teleportacji zera bądź jedności, wartości parametru theta powinny przyjmować wartości

$$\Theta^0=\frac{(4k-1)\pi}{4},\quad \Theta^1=\frac{(4k+1)\pi}{4}\quad dla\quad k\in Z. \qquad (2.5)$$

Jednakże należy odpowiednio dobrać parametr obrotu theta. Zbyt duży obrót powoduje zbyt znaczące osłabienie splątania w kierunku stanów zero bądź jeden w zależności od doboru wartości theta.



Rys. X2. Wykresy prawdopodobieństwa zmierzenia stanu zero bądź jeden, podczas teleportacji stanu zero obwodem z Rys. X1
Fig. X2. Figure of probability values of measure zero and one states at the teleportation of the zero state using circuit from Fig. X1



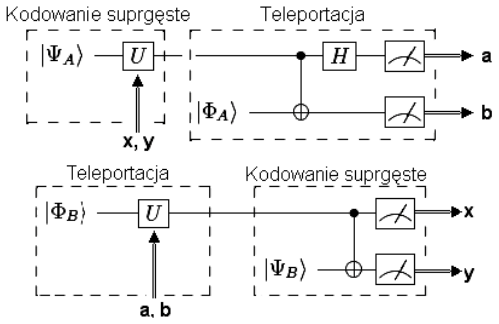
Rys. X3. Wykres prawdopodobieństwa zmierzenia stanu zero oraz jeden podczas teleportacji stanu zero dla zmieniających się wartości parametru theta w zakresie od zera do dwóch z krokiem 0.2 (kolor czerwony to wartości dla zera, niebieski dla jedności)
Fig. X3. Figure of probability values of measure zero and one states at the teleportation of the state zero. Probability values depend on the value of theta parameter which is varying from zero to two with step 0.2 (red color denotes the probability of zero and the blue of one)

3. Protokół transferu klucza w kanale kwantowym

Głównym problemem kryptografii jest kwestia bezpiecznej akwizycji klucza. Zastosowanie statystycznej teleportacji pozwala nam na ustanowienie jednorazowego klucza potrzebnego np. w protokole Vernama, który jak wiemy gwarantuje pełne bezpieczeństwo. Podstawowym rozpatrywanym atakiem jest tzw. atak 'man in the middle', gdzie podsłuchujący może kontrolować cały transfer danych, tj. dokonywać pomiarów na wszystkich przesyłanych qubitach, a także symulowania przed każdą ze stron bycia drugą stroną protokołu. W przypadku tego protokołu nie mamy jednak żadnego fizycznego transferu. Strony są od siebie odseparowane i dokonują wyłącznie pomiarów na posiadanych już qubitach. W tej sytuacji możliwy jest jedynie atak polegający na przejęciu lub podmianie przez ewentualnego podsłuchiwacza splątanych qubitów należących do odbiorcy. Jednak w tej sytuacji odbiorca po otrzymaniu klucza i próbie odszyfrowania przykładowej wiadomości testowej będzie miał świadomość oszustwa i o ile będzie istniał kanał zwrotny, będzie on mógł powiadomić o tym nadawcę. Przypadek w którym podsłuchiwacz może pozostać niewidzialny wymaga, aby przejął on i podmienił własnymi zarówno wszystkie splątane końcówki nadawcy jak i odbiorcy. Wtedy nadawca komunikowałby się z podsłuchiwaczem, a dopiero on komunikowałby się z odbiorcą. Wydaje się trudne choćby ze względu na w domyśle dowolnie wielką przestrzeń dzielącą strony. W tym przypadku ani wiadomości testowe, ani kanał zwrotny nie będą pomocne w wykryciu podsłuchu. Pomocne natomiast będzie wstępne dzielenie przez strony tajemnicy przypisanej do splątanych qubitów odnośnie bazy lub serii baz pomiarowych, a także informacji o ilości teleportowanych qubitów dla ustalenia pojedynczego bitu klucza.

W ogólnym przypadku, po przesłaniu klucza, wiadomość i tak przesyłana jest kanałem klasycznym. Ma to znaczenie w sytuacji, gdy mamy znaczne odległości pomiędzy nadawcą, a odbiorcą, lub

nawet nie wiemy gdzie w danej chwili znajduje się odbiorca. Stąd też idea, aby zaszyfrowaną wiadomość przesyłać kwantowo. W tym przypadku każde dwa klasyczne bity wiadomości kodowane są za pomocą kwantowego kodowania supergęstego do postaci określonego stanu qubitu. Następnie qubit ten klasycznym protokołem teleportowany jest do odbiorcy, przy czym informacje, które należałoby przesłać klasycznie będą również teleportowane, tyle że protokołem probabilistycznym. Dzięki temu nie mamy potrzeby oczekiwania na dotarcie klasycznej informacji. Posiadane przez strony splątane qubity pełnią w tym przypadku rolę klucza. Schemat takiej transmisji przedstawiony jest na Rys. X4. Dwa bity x i y, które zamierzamy przesłać definiują operację unitarną, którą zgodnie ze schematem kodowania supergęstego wykonujemy na pierwszym qubicie splątanym nadawcy $|\Psi_A\rangle$, a następnie otrzymany stan teleportujemy do odbiorcy z wykorzystaniem drugiego qubitu splątanego nadawcy $|\Phi_A\rangle$. Potrzebne odbiorcy do zakończenia teleportacji bity a i b przesyłamy za tu pomocą teleportacji probabilistycznej.



Rys. X4. Obwód nadawczy i obwód odbiorczy protokołu transferu.
Fig. X4. Sender and receiver circuits for the transfer protocol.

4. Posumowanie

Mimo nieustannego postępu zarówno na poziomie teoretycznym jak i na poziomie eksperymentalnym w dziedzinie teleportacji stanów kwantowych [13,14,15,16,,17,18], mało się pisze o możliwych zastosowaniach tego transferu w dziedzinie istniejących obecnie technologii. Praktyczna implementacja zaproponowanych w tym artykule probabilistycznych protokołów transferu klasycznych bitów przy użyciu kwantowych kanałów otworzyłaby drogę do wielu praktycznych zastosowań teleportacji w dzisiaj stosowanej technologii informatycznej.

Dotyczy to zwłaszcza tak nabierających na ważności dziedzin jak ochrona danych i bezpieczny transfer informacji [19,20]. Jedno z możliwych tego rodzaju zastosowań opisaliśmy powyżej opisując pewne nowe koncepcje w zakresie kwantowej kryptografii, a zwłaszcza bezpiecznych transferów klucza jak i samej informacji klasycznej. Oczywiście droga do implementacji opisanych zastosowań do praktyki dnia powszedniego wydaje się aczkolwiek najeżona wieloma problemami, to jednak nie beznadziejna.

W przygotowanym przez nas artykule [21] opisujemy szeroko cała klasę tego rodzaju stochastycznej transmisji klasycznej informacji w kanałach kwantowych, a także przedstawiamy całe spectrum fascynujących zastosowań do klasycznej informatyki.

5. Literatura

[1] Einstein A., Podolsky B., Rosen N.: Can quantum-mechanical description of physical reality be considered complete ?, Phys. Rev. 47, p.777, (1935).
[2] Bell J.S.: Speakable and unspeakable in quantum mechanics, Cambridge University Press, Cambridge, (1987).
[3] Aspect A., Dalibard, Roger G.: Experimental Test of Bell's Inequalities Using Time-Varying Analyzers, Phys. Rev. Lett. 49, 1804, (1982).
[4] Cartwright J.: Quantum physics says goodbye to reality, physicsworld.com, (2007).
[5] Gill R. D.: Time, finite statistics, and Bell's fifth position, Foundations of probability and physics, pp. 179–206, Vaxjio Univ. Press, (2003).
[6] Bennett C.H., Brassard G., Crepeau C., Jozsa R., Peres A. and Wooters W.K.: Teleporting an unknown state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett., Vol. 70, pp. 1895-1899, (1993).
[7] Werner R.F.: All teleportation and dense coding schemes, J. Phys. A: Math. Gen. 34, pp. 7081-7094, (2001).
[8] Bouwmeester D., Ekert A., Zelinger A., Editors: The Physics of Quantum Information: quantum cryptography, quantum teleportation, quantum computation, Elsevier, (2000).
[9] Sherson J.F., Krauter H., Olsson R.K, Julsgaard B, Hammerer K, Cirac I., Polzik E.S.: Quantum teleportation between light and matter, Nature 443, pp. 557-560, (2006).
[10] Nielsen M.A., Chuang I.L.: Quantum Computation and Quantum Information, Cambridge U. Press, New York, (2000).
[11] Furusawa A., Sorensen J. L., Braustein S. L., Fuchs C. A., Kimble H. J., Polzik E. S.: Science 282, 706, (1998).
[12] Bennett C. H., Bernstein H. J., Popescu S., Schumacher B.: Phys. Rev. A 53, 2046, (1996).
[13] Agrawal P., Pati A. K., J. Opt. B: Quant. Semi. Opt. 6, S844, (2004).
[14] Carvalho C.R., Guerra E.S., Jalbert G., Garreau J.C.: Nonprobabilistic teleportation of field state via cavity QED, Journal of Physics B: Atomic, Molecular and Optical Physics 40, pp. 1271-1282, (2007).
[15] Zhang Q., Goebel A., Wagenknecht C., Chen Y., Zhao B., Yang T., Mair A., Schmiedmayer J., Pan J.:Eperimental Quantum Teleportation of a Two-Qubit Composite System, Nature Physics 2, pp. 678-682 (2006).
[16] Hammerer K., Polzik E.S., Cirac J.I.: High fidelity teleportation between light and atoms, PRA 74, 064301 (2007).
[17] Kondo Y.: Quantum Teleportation without Irreversible Detection: NMR-Experiment, J. Phys. Soc. Jpn. 76, 104004 (2007).
[18] Yonezawa H., Braunstein S.L., Furusawa A.:Experimental Demonstration of Quantum Teleportation of Broadband Squeezing, Phys. Rev. Lett. 99, 110503 (2007).
[19] Kościelny C.: A New Approach to the Elgamal Encryption Scheme, Int. J. Appl. Math. Comput. Sci., Vol. 14, No. 2, pp. 265-267, (2004).
[20] Jankowska B.M.: Howto Secure a High Quality Knowledge Base in a Rule-Based System with Uncertainty?, Int. J. Appl. Math. Comput. Sci., Vol. 16, No. 2, pp. 251-262, (2006).
[21] Gielerak R., Sawerwain M., Ratajczak P., in preparation.

Title: Probabilistic classical information transfer protocol in quantum channel

---

Artykuł recenzowany