РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 621.3 (045)
DOI https://doi.org/10.32782/2663-5941/2022.5/01

Білаш Б.О.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Лисенко О.М.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

БЕЗПОМИЛКОВЕ ВИЗНАЧЕННЯ КВАНТОВОГО СТАНУ БЕЛЛА У КВАНТОВІЙ КРИПТОГРАФІЇ

У статті розглянуто один із найбільш перспективних методів сучасної квантової криптографії – метод квантового розподілу ключів QKD (Quantum Key Distribution) на основі пар станів Белла квантової заплутаності. Запропоновано узагальнену квантову схему для визначення чотирьох станів Белла третіми особами без знищення оригінального стану, яка дозволяє третім сторонам взаємодіяти окремо з кожним кубітом пари Белла. При цьому вирішувалися два завдання одночасно: перевірка умови «визначення стану» Белла, тобто чи можливо отримати повну інформацію про оригінальні кубіти стану Белла від довірених сторін; з іншого боку, перевірка умови «неруйнівний стан», тобто, чи можливо не руйнувати початковий стан Белла. Оскільки кожен кубіт Белла надсилається окремим шляхом, що робить можливість відстані між кубітами безкінечно великою, це не дозволило застосування відомої схеми, запропонованої Гуптою та ін. Тому використано перевагу заздалегідь підготовлених для взаємодії заплутаних станів, які вперше були розглянуті Пейджом та ін. і розвинуті в цій статті. Для кожного кубіту окремо визначається умова "фази" та "парності", для яких створені окремі квантові пари між третіми сторонами. Через те, що кубіти стану Белла можуть знаходитись далеко один від одного при передачі інформації, треті сторони не можуть напряму взаємодіяти з їх кубітами, але можуть обмінюватись класичними бітами після вимірювання своїх кубітів. Для повноцінного отримання інформації третіми сторонами в статті запропоновано нову універсальну схему телепортації квантових вентилів, яка була спрощена та адаптована для умов визначення станів Белла. Зазначене рішення забезпечує 100% ймовірність визначення будь-якого стану Белла для ідеального випадку без шумів. Дана схема реалізована та апробована на квантовому комп'ютері IonQ.

Ключові слова: *квантові обчислення, квантова криптографія, квантовий криптоаналіз, стан Белла, кубіти.*

Постановка проблеми. Загально відомо, що вирішення проблеми збереження даних завжди було актуальним для людства. Особливе місце в цьому займає збереження інформації при спілкуванні між двома сторонами. Для цього людська спільнота використовує криптографію, де дві довірені сторони кодують інформацію, яка представлена наборами класичних бітів «0» і «1», іншим набором класичних бітів. У квантовій криптографії аналогічно класичній дві довірені сторони обмінюються інформацією, яка представлена замість наборів класичних бітів квантовими бітами (кубітами). Іншими словами, у квантовій криптографії кубіти використовуються не як джерела інформації, а лише як спосіб кодування класичних наборів бітів і як носії інформації. Протягом останніх десятиліть одним із найбільш перспективних методів сучасної квантової криптографії є метод квантового розповсюдження ключів QKD (Quantum Key Distribution), заснований на законах квантової механіки. Першим відомим протоколом QKD є BB84 [1], який використовує для кодування даних чотири квантових стани фотонів на основі двох базисів з використанням поляризаційних станів світла. Інший відомий протокол E91 [2] заснований на квантовій заплутаності [3, 4]. У цій роботі нас буде цікавити квантовий розподіл ключів QKD на основі пар станів

Белла квантової заплутаності. Однак, насамперед, необхідно перевірити, чи справді ці пари захищені від втручання, іншими словами, необхідно провести квантовий криптоаналіз. Згідно з теоремою про відсутність клонування [5] неможливо скопіювати будь-який квантовий стан. Якщо дві довірені сторони збираються обмінюватися інформацією, вони можуть закодувати класичний біт «0» або «1» у певні окремі кубіти з різними станами. Однак, якщо третя, ненадійна, сторона знає метод кодування, вона може декодувати довірений кубіт, щоб визначити вихідний стан, при цьому відсутня квантова перевага. Однак, її можна отримати за допомогою заплутаних станів. Якщо довірені сторони використовують 2 кубіти для кодування 2 класичних бітів, вони можуть ділитися цими кубітами різними фізичними шляхами. Ці шляхи можуть бути нескінченно далекі один від одного. Одним із можливих заплутаних станів є стани Белла, які представлені двома кубітами. Кожні два класичні біти можна перевести в квантову пару Белла. Щоб визначити ці стани Белла, довірені сторони повинні використовувати квантове вимірювання стану Белла (Bell-state measurement, BSM), в результаті чого вони можуть отримати класичні біти. Навіть якщо третя сторона знає про метод кодування, їй потрібно використовувати BSM для визначення стану Белла, після чого стан Белла буде знищено. З іншого боку, якщо третя сторона намагається будь-яким чином вплинути на стани Белла, вона може їх знищити, про що стане відомо довіреним особам. Однак третя сторона може спробувати визначити стан Белла, не руйнуючи його шляхом взаємодії з кубітами стану Белла. У цій роботі авторами розглянуто цей сценарій, а саме, чи можливо отримати інформацію про стани Белла без їх знищення третіми особами таким чином, щоб при цьому довірені сторони не дізналися про це. Тому у подальшому вирішуватимуться два завдання одночасно: перевірка умови «визначення стану Белла», тобто чи можливо отримати повну інформацію про оригінальні кубіти стану Белла від довірених сторін; з іншого боку, перевірка умови «неруйнівний стан», тобто, чи можливо не руйнувати початковий стан Белла.

Аналіз останніх досліджень і публікацій. У 2005 році Гуптою та ін. було запропоновано квантову схему для вирішення цієї задачі [6, 7], яка була експериментально апробована [8]. У цих роботах автори пропонують використовувати 2 кубіти для взаємодії з парами стану Белла. Кожен кубіт використовується для визначення «парності» та «фазової» різниці між двома кубітами стану Белла. Поєднуючи результати взаємодії цих двох кубітів, можна визначити будь-який стан Белла, не руйнуючи його. Кожен перевірочний кубіт взаємодіє з обома кубітами стану Белла. В подальшому у цій роботі буде показано принципово інші підхід та схему визначення станів Белла, згідно яким кожен кубіт з довіреної пари стану Белла взаємодіятиме з перевірочними кубітами, підготовленими спеціально для нього.

У 2020 році Пейдж та ін. запропонували квантові ігри для демонстрації некласичних властивостей станів квантової заплутаності, які називаються Delocalized-Interactions [9]. Зокрема, ігровий сценарій «розрізнення стану Белла» (Bell-Discrimination, BD) можна використовувати для визначення певного стану Белла. Основна ідея полягає в тому, щоб продемонструвати наявність або відсутність кубіта (логічний «0» або «1»). Таким чином, автори використовують різницю парності між станами Белла. Однак, вони не розрізняють різницю фаз між станами Белла, що не входило в їх завдання.

Постановка завдання. У цій роботі авторами пропонується інший підхід для визначення станів Белла без їх руйнування. Два кубіти, які містять будь-який стан Белла, розділені просторово. Для визначення станів Белла пропонується використання двох додаткових наборів кубітів, які будуть окремо взаємодіяти лише з одним кубітом стану Белла. Ці набори кубітів не можуть знищувати початкові стани Белла, тобто вони повинні відповідати умові «неруйнівний стан». Крім того, вони не можуть взаємодіяти один з одним, однак, після вимірювання класичні біти можуть бути спільно використані з метою визначення, який стан Белла був застосований, тобто вони повинні відповідати умові «розрізнення станів Белла». Цей підхід в подальшому буде реалізовано авторами у вигляді квантової схеми, яка пройде також апробацію на реальному квантовому комп'ютері IonQ. Це може також стати і основою для розробки нових протоколів квантового зв'язку.

Таким чином, підсумовуючи, зазначимо, що подальший сценарій реалізації в цій роботі запропонованого авторами підходу полягатиме спочатку у висвітленні його відрізняльних особливостей від відомого, створенні авторами квантової схеми його реалізації, яка використовуватиме кілька попередньо спільних заплутаних станів залежно від умов «парності» та «фази». При цьому кожна із умов буде розглянута авторами в окремому підрозділі. Також будуть висвітлені обмеження, які виникли під час створення

квантової схеми і показано, як телепортація квантових вентилів допоможе подолати ці обмеження шляхом впровадження схеми телепортації квантових вентилів до квантової схеми згідно основного підходу. Після цього буде викладено і обговорено отримані результати реалізації запропонованого рішення з використанням квантового комп'ютера IonQ.

Виклад основного матеріалу. Основний матеріал буде містити наступні підрозділи: аналіз існуючого та запропонованого сценаріїв вирішення задачі, узагальнена квантова схема, визначення умови "парності", визначення умови "фази", квантова телепортація CNOT вентиля, спрощення запропонованої схеми та результати дослідження.

Аналіз. Тепер проведемо аналіз існуючого та запропонованого сценаріїв для вирішення задачі, яка буде розв'язуватися в цій роботі. Розглянемо дві сторони, Чарлі (Charlie, C) і Девід (David, D). C хоче надіслати інформацію, представлену класичними бітами, до D. Як показано у вступній частині, C використовуватиме квантовий розподіл ключів, розділивши свій набір бітів по два та закодувавши їх у пари Белла, після чого надсилає кожний кубіт до D різними шляхами. Стан Белла є найпростішим, але водночас максимально заплутаним станом [3, 4]. Для його визначення необхідно провести вимірювання стану Белла (BSM), після чого будь-якому з можливих станів Белла буде відповідати певна комбінація двох класичних бітів. Відповідно до [5] будь-який квантовий стан, у тому числі стан Белла, не можна скопіювати. У цьому випадку, якщо третя, ненадійна сторона, намагається отримати інформацію від C, ця сторона повинна виконати процедуру вимірювання BSM, отримати класичні біти, підготувати новий стан Белла і надіслати його D. У цьому сценарії ненадійна сторона повинна мати два кубіти стану Белла разом, тобто ці кубіти повинні бути досить близько один до одного. В іншому випадку третя сторона не може отримати будь-яку інформацію про стан Белла. Згідно запропонованому сценарію C надсилає свої кубіти до D окремо двома різними шляхами. Відстань між цими шляхами може бути нескінченно великою. Однак, врешті-решт, D повинен отримати кубіти C з різних шляхів і виконати вимірювання стану Белла (BSM), щоб визначити класичні біти. Тоді, якщо два кубіти нескінченно віддалені один від одного, ненадійна сторона не може взаємодіяти з двома кубітами стану Белла разом і одночасно. Ще однією складовою вирішуваної задачі для довірених сторін є збереження початкового стану Белла без його руйнування. З [6, 7] вже відомо, що будь-яка третя сторона може отримати інформацію про стан Белла, не руйнуючи його. На відміну від наведеного вище відомого сценарію згідно запропонованому C надсилає свої кубіти до D окремо двома різними шляхами. У ідеальному випадку без шумів, якщо цей стан Белла не було знищено третьою стороною, після процедури вимірювання BSM класичні біти у D будуть такими ж, як і біти, закодовані C. Для цього випадку схему, запропоновану Гуптою [6, 7], неможливо реалізувати, оскільки перевіряючі кубіти повинні взаємодіяти з обома кубітами стану Белла разом. Однак, кожен кубіт C із пари стану Белла йде до D різними нескінченно розділеними шляхами. Згідно запропонованому сценарію представимо ще дві сторони, Алісу (Alice, A) і Боба (Bob, B), які можуть взаємодіяти лише з одним кубітом стану Белла C відповідно. Розглянемо ситуацію, наведену на Рис. 1, де A і B можуть мати свої кубіти і взаємодіяти з кубітами C незалежно, але вони не хочуть порушувати вихідний стан C. Крім того, A і B не можуть взаємодіяти між своїми кубітами під час процесу, але вони можуть порівнювати свої результати в класичних бітах після вимірювання своїх кубітів. Після взаємодії D отримує кубіти C і реалізує процедуру вимірювання BSM для кубітів C, щоб розрізнити та визначити вихідні класичні біти C.

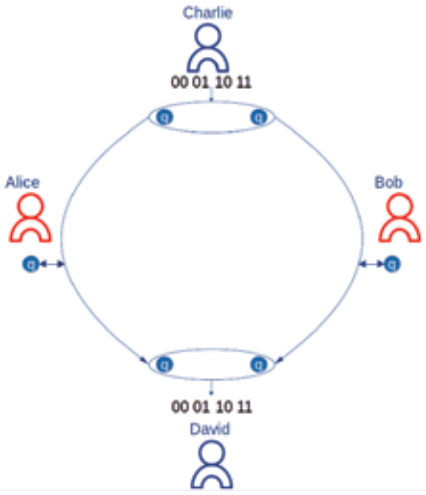

Рис. 1. Схематичне зображення взаємодії сторін A – D згідно запропонованому сценарію

Очевидно, що A і B заборонено копіювати стани кубітів C згідно з теоремою про заборону клонування [5]. Уявімо наступну ситуацію. A і B хочуть перевірити стан Белла C. Їх перевіряючі кубіти певним чином взаємодіятимуть із кубітами стану Белла C. Якщо розглянути випадок парності стану Белла C, тобто, він знаходиться в станах $|\Phi^+\rangle$, $|\Phi^-\rangle$ (парність), кожен перевіряючий

кубіт з A і B залишиться незмінним. Однак, якщо стан Белла знаходиться в станах $|\Psi^+\rangle$, $|\Psi^-\rangle$ (непарний паритет), один перевіряючий кубіт A або B буде випадковим чином перевернуто. Аналогічно, якщо A і B хочуть перевірити фазовий стан стану Белла, який знаходиться в станах $|\Phi^+\rangle$, $|\Psi^+\rangle$, тобто кубіти знаходяться в одній фазі, будь-які перевіряючі кубіти A і B залишаться незмінними. Однак, якщо стан Белла знаходиться в станах $|\Phi^-\rangle$, $|\Psi^-\rangle$, тобто кубіти знаходяться в різних фазах, один перевіряючий кубіт A або B буде перевернуто випадковим чином. Ця квантова особливість заснована на певних залежностях між двома кубітами стану Белла. У [9] автори показали потужність попередньо заплутаних квантових станів. A і B можуть підготувати між собою попередньо спільні заплутані стани. Після цього A і B незалежно взаємодіють між своїми кубітами та кубітами C. У нашому випадку A і B використовують більше одного попереднього спільного заплутаного стану. Наприклад, перша пара кубітів із попередньо спільним заплутаним станом може визначати умову «парності», друга пара може визначати умову «фази». Таким чином, A і B можуть реалізувати визначення стану Белла. Однак, оригінальні кубіти стану Белла C неможливо виміряти, змінити або знищити. Тобто, має бути виконана умова «неруйнівний стан». Після взаємодії A і B можуть вимірювати свої кубіти та обмінюватися виміряними результатами у формі класичних бітів для визначення стану Белла C. З ансамблю всіх можливих комбінацій двох класичних бітів набори певних комбінацій бітів відповідатимуть певним станам Белла. Ці набори будуть представлені пізніше, оскільки встановлення того, як біти будуть обмінюватися між A і B для визначення стану Белла C виходить за рамки цієї роботи. Паралельно вихідні кубіти C досягнуть D без втрати станів. Далі детально пояснимо, як реалізувати цей сценарій.

Узагальнена квантова схема. Представимо розглянутий вище сценарій визначення чотирьох станів Белла за окремими сторонами A і B. Спочатку розділимо запропоновану узагальнену квантову схему на дві незалежні складові, перша з яких визначає умову «парності» для кубітів стану Белла C, а друга – «фазові» умови. Однак, обидві складові мають однакову послідовність дій, наведену на рис. 2.

Крок 1 є підготовчим для A і B, які створюють деякий попередньо спільний заплутаний стан для дослідження стану Белла C. На рис. 2. між A і B є стан Белла $|\Phi^+\rangle$, при цьому на кроці 2, наприклад, C створює стан Белла $|\Phi^+\rangle$. C може підготувати будь-яку іншу пару станів Белла, яка залежить від 2-бітної класичної інформації, яку вона хоче надіслати D. На кроці 3 A і B певним чином взаємодіють з кубітами C, щоб перевірити, який стан Белла надсилається без визначення. Детальніше це буде показано пізніше. На кроці 4 D виконує процедуру вимірювання BSM, щоб визначити, який стан Белла було надіслано з C.

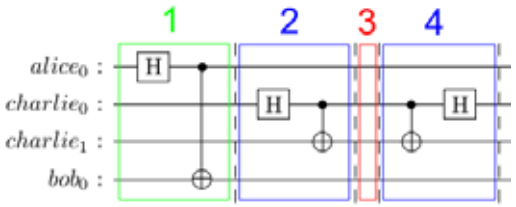

Рис. 2. Запропонована узагальнена схема визначення станів Белла

Спочатку детально розглянемо умову “парності”

Визначення умови “парності”. На рис. 3 представлено схему для визначення умови «парності» для кубітів стану Белла C з [9].

Надалі будемо представляти квантовий стан наступним чином: $|q_3q_2q_1q_0\rangle$ позначатиме, що q_0

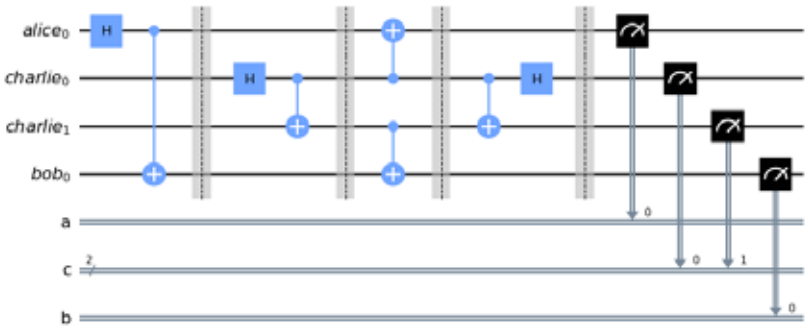

Рис. 3. Схема для визначення умови “парності” [9]

є кубіт A, q_1, q_2 є кубіти C, q_3 є кубіт B відповідно. На кроці 1, коли A і B готують попередньо спільні заплутані стани, тоді глобальний стан буде $\frac{(|0000\rangle+|1001\rangle)}{\sqrt{2}}$. На кроці 2 C готує свій стан Белла. Спочатку розглянемо випадок, коли C готує $|\Phi^+\rangle$ стан Белла. Тоді глобальний стан буде $\frac{(|0000\rangle+|1001\rangle+|1111\rangle+|0110\rangle)}{2}$. На кроці 3 A і B застосовують операцію CNOT між кожним кубітом C у стані Белла та їхніми кубітами перевірки. Тут кубіти C діють як контрольні кубіти. Тоді глобальний стан буде наступним (1):

$$\frac{(|0000\rangle+|1001\rangle+|1111\rangle+|0110\rangle)}{2} \quad (1)$$

Цей результат є точно таким же, як і на попередньому кроці. Потім, коли D виконує вимірювання стану Белла (BSM), результат залишатиметься таким же, як і початковий. Після вимірювання A і B матимуть з 50% ймовірністю результат вимірювання $|00\rangle$ або $|11\rangle$ станів. Той самий результат для випадку коли C готує стан $|\Phi^-\rangle$.

Розглянемо тепер іншу ситуацію, коли C надсилає стан Белла $|\Psi^+\rangle$. Тоді після кроку 2 глобальний стан буде таким: $\frac{(|0010\rangle+|1011\rangle+|0100\rangle+|1101\rangle)}{2}$. Потім після взаємодії між станом Белла C і кубітами A, B за допомогою операції CNOT результуючий стан виглядає наступним чином (2):

$$\frac{(|0011\rangle+|1010\rangle+|1100\rangle+|0101\rangle)}{2} \quad (2)$$

Варто зазначити, що початкові кубіти C залишаються незмінними і коли D виконує процедуру вимірювання BSM, він матиме той самий результат, що й відправлений від C. Примітно, що кубіти A і B змінились. Вимірюючи свої кубіти, A і B мають 50% ймовірність отримати стан $|01\rangle$ або $|10\rangle$. A і B отримають такий самий результат, якщо C підготує стан $|\Psi^-\rangle$. Різні вихідні дані, які A і B отримують для стану Белла з різною парністю, дозволяють A і B розрізнити, чи є стан Белла C парним чи непарним.

Однак, A і B не можуть розрізнити, яку фазу мають стани Белла, тобто вони не можуть розрізнити між $|\Psi^+\rangle$ і $|\Psi^-\rangle$ та між $|\Phi^+\rangle$ і $|\Phi^-\rangle$. Щоб вирішити це завдання, вводимо додатковий попередньо спільний заплутаний стан між A і B для роботи з умовою фази стану Белла.

Визначення умови “фази”.

Розглянемо, як за станом Белла визначити стан «фази». Схема, яка реалізує це, наведена на рис. 4. Якщо C надсилає стан $|\Phi^+\rangle$, глобальний стан після кроку 2 буде таким (3):

$$\frac{(|0000\rangle+|1001\rangle+|0110\rangle+|1111\rangle)}{2} \quad (3)$$

У випадку, якщо C надсилає $|\Phi^-\rangle$ стан, глобальний стан після кроку 2 буде наступним (4):

$$\frac{(|0000\rangle+|1001\rangle-|0110\rangle-|1111\rangle)}{2} \quad (4)$$

Тоді, якщо A і B виконують операції CNOT між своїми кубітами як контрольними кубітами і кубітами C, які відрізняються від кроку 3 при визначенні парності, вирази (3), (4) зміняться на відповідні (5), (6) глобальні стани наступним чином:

$$\frac{(|0000\rangle+|1111\rangle+|0110\rangle+|1001\rangle)}{2} \quad (5)$$

$$\frac{(|0000\rangle+|1111\rangle-|0110\rangle-|1001\rangle)}{2} \quad (6)$$

Вираз (5) повністю співпадає з виразом (3), однак, вираз (6) відрізняється від виразу (4). Це вказує на те, що запропонована схема може розрізняти різні фазові умови заданих двох станів Белла. Для випадку (5), коли D виконує процедуру вимірювання BSM, результат є таким самим для випадку «парності». Однак, випадок (6) є більш цікавим. Коли D виконує процедуру вимірювання BSM (але без фізичного вимірювання кубітів), він матиме оригінальний стан Белла $|\Phi^-\rangle$, який підготувала C. Глобальний стан буде наступним: $\frac{(|0010\rangle-|1011\rangle)}{\sqrt{2}}$. Після вимірювання кубітів D він отри-

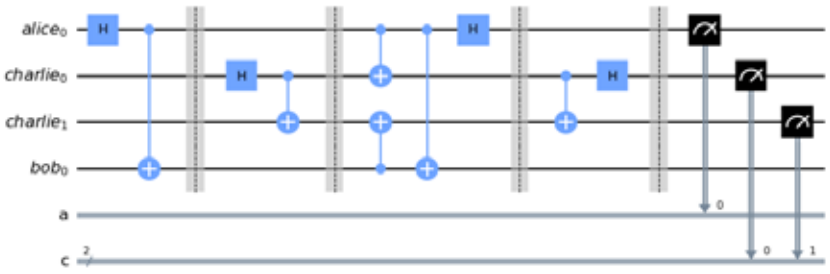

Рис. 4. Схема для визначення умови “фази”

має оригінальні класичні біти, які C хотіла надіслати. Тоді після видалення кубітів від C, кубіти A і B можна представити наступним чином (7):

$$\frac{(|00\rangle - |11\rangle)}{\sqrt{2}} \quad (7)$$

Як видно, цей стан – це саме $|\Phi^-\rangle$ стан Белла. І очевидно, що для випадку виразу (5) A і B матимуть стан Белла $|\Phi^+\rangle$ після того, як D виміряє стан, який він отримав (8):

$$\frac{(|00\rangle + |11\rangle)}{\sqrt{2}} \quad (8)$$

Щоб точно розрізнити ці два стани, A і B повинні виконати процедуру вимірювання BSM [4, 10], що також виконується на кроці 3 (рис. 4). Іншим важливим моментом є те, що B не обов'язково вимірювати свій кубіт, оскільки результатом вимірювання завжди був би стан $|0\rangle$. Отже, щоб визначити стан «фази», достатньо виміряти лише кубіт A.

Комбінуючи схеми на рис. 3 та рис. 4, A і B можуть точно розрізнити будь-який стан Белла, не руйнуючи його, що відображено на рис. 5.

Однак, раніше було висловлено припущення, що A і B не можуть безпосередньо взаємодіяти один з одним. Тоді A і B не можуть виконувати процедуру вимірювання BSM між своїми кубітами, як запропоновано вище. Щоб вирішити цю проблему необхідно модифікувати запропоновану схему, щоб не мати взаємодії після початкового спільного використання заплутаних пар.

Квантова телепортація CNOT вентиля. На відміну від стану «парності», який можна спостерігати в класичному світі, стан «фази» притаманний лише квантовому світу. Вирази (7) і (8) мають однакові власні вектори, але з різними власними значеннями. Після вимірювання ці вектори стану згорнуться до тих самих класичних бітів.

Щоб визначити різницю «фаз», як було сказано в попередньому підрозділі, A і B повинні виконати процедуру вимірювання BSM між своїми кубітами [4, 10]. Однак, їхні кубіти не можуть взаємодіяти один з одним напряму відповідно до умов, які були зазначеніі раніше. Але після вимірювання A і B можуть обмінятися своїми класичними бітами. Як цю перевагу можна реалізувати? A і B просто повинні виконувати CNOT між своїми кубітами.

У [11] автори показали, як може бути реалізована квантова телепортація. Кінцева її мета полягає в тому, щоб реалізувати взаємодію між двома різними кубітами та перенести результат взаємодії на інші кубіти. Для цієї телепортації автори вимірюють кубіти і за класичним результатом згортання змінюють інші кубіти так само, як телепортація квантового стану [10]. Ця концепція може бути використана для запропонованого методу 2 шляхом обміну класичними бітами між A і B. Аліса та Боб можуть реалізувати вентиль CNOT між собою як квантову телепортацію шляхом вимірювання їхніх кубітів і впливу на інші кубіти, де достатньо для обміну лише класичними бітами. У цьому підрозділі пропонується нова квантова схема, яка використовує телепортацію квантових вентилів. A має підготувати ще два допоміжні кубіти, які отримають результат операції CNOT між перевіркою кубітів на стан «фази». У цьому випадку B буде надсилати A лише класичні біти. Нова схема телепортації воріт CNOT наведена на рис. 6 та реалізована шляхом модифікації оригінальної схеми (рис. 5). 6 кубітів, які необхідні для телепортації квантових воріт між A і B, розділені на 3 кубіти для кожної сторони. На кроці 1 готуються дві заплутані пари кубітів між A і B. Для кращої читабельності перша пара кубітів, яка перевіряє умову «парності», розташована ближче до кубітів C, тобто для кубітів $alice_3$ і bob_0

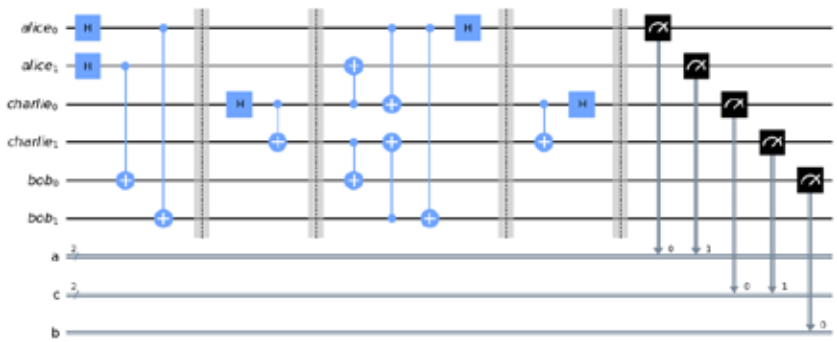

Рис. 5. Схема для повного визначення стану Белла

відповідно. Тоді кубіти, які перевіряють умову «фази», будуть розміщені до найдальших кубітів, тобто для кубітів $alice_0$ і bob_3 відповідно. На кроці 2 готуються кубіти для квантової телепортації. A і B хочуть телепортувати результат взаємодії з кубітами C до інших кубітів A і B відповідно. Результат телепортації квантових воріт буде на кубітах $alice_2$ і bob_1. На кроці 3 C готує будь-який стан Белла, а потім надсилає його до D. На кроці 4 A і B взаємодіють з кубітами C незалежно. Кубіти $alice_3$ і bob_0 взаємодіють, щоб визначити різницю «парності». Кубіти $alice_0$ і bob_3 взаємодіють, щоб визначити різницю «фаз». На кроці 5 реалізується квантова телепортація з вимірювальними кубітами. Після цього застосовуються квантові вентилі «X» і «Z» в залежності від результатів вимірювання. Також Аліса задіює квантовий вентиль «H» до свого кубіта $alice_2$. На кроці 6 і 7 D отримує кубіти C і виконує процедуру вимірювання BSM. Біти результату будуть такими ж, як і закодовані біти C. На останньому кроці 7 A і B вимірюють свої кубіти. Вимірювання може виконуватись в будь-який період часу після взаємодії між кубітами A і B і C відповідно. Результат не зміниться. Крім того, згідно з оригінальною схемою на рис. 5, B не потрібно вимірювати кубіт bob_2.

Таким чином, модифікована оригінальна схема вирішує проблему. A та B не потрібно взаємодіяти один з одним, досить обмінятися лише класичними бітами, щоб розпізнати оригінальний стан C.

Однак, для прямої роботи квантових вентилів «Z» і «X», які контролюються виходами вимірювань, потрібен зв'язок між A і B. Наступним кроком буде спрощення запропонованої схеми для вирішення цієї проблеми.

Спрощення запропонованої схеми. Насправді запропоновану квантову телепортацію CNOT вентиля важко застосувати в реальній фізичній системі. Коли B вимірює свої кубіти та надсилає класичні біти A, вона, у свою чергу, повинна постійно зберігати свої кубіти. Крім того, фізично важко реалізувати квантові вентилі в залежності від класичних бітів. Це вимагає складної архітектури. Зважаючи на ці обмеження, більш простим способом є зміна вихідної частини схеми (рис. 6) і визначення бітів C шляхом її модифікації.

Давайте нагадаємо, чому в роботі використовується квантова телепортація – є потреба у визначенні лише «фазової» умови після взаємодії з кубітами C без нелокальної взаємодії між A і B. Умова «парності» вже виникає в інших кубітах. Однак, запропонована на рис. 6 схема телепортації квантових воріт є універсальною та забезпечує обидві умови «парності» і «фази». Тому доцільним

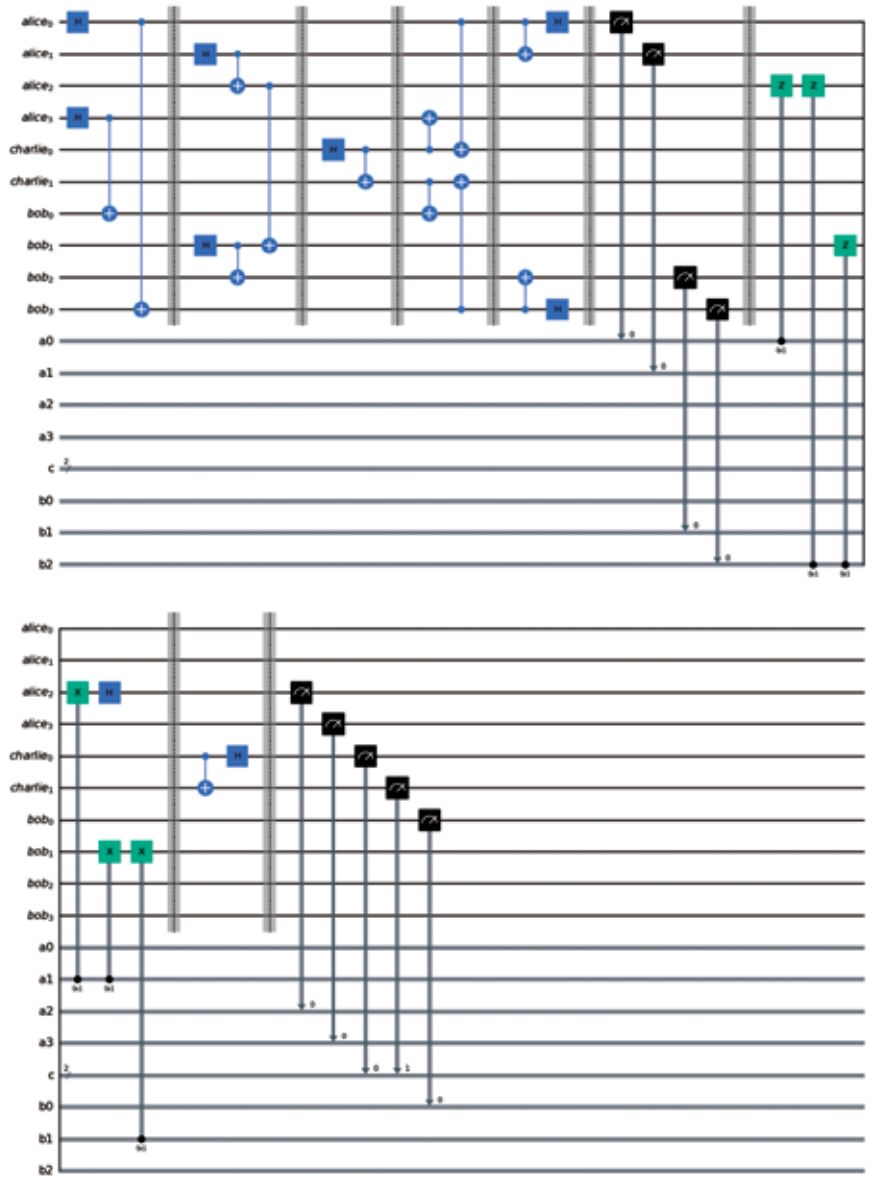

Рис. 6. Схема із застосуванням квантової телепортації CNOT вентиля

є «очищення» частини умов «парності» з квантової схеми. У цьому випадку A і B не потрібно вимірювати кубіти $alice_1$ і bob_2 для визначення умови «парності» і не використовувати квантові ворота «X» після нього.

Як було зазначено раніше, лише кубіт $alice_2$ показує «фазову» різницю між кубітами стану Белла C. У той же час кубіт bob_1 буде кожного разу в стані «0». Тоді B не потрібно використовувати bob_1 у своєму результаті, він може видалити квантовий вентиль «Z» для цього кубіта і не повинен його вимірювати.

На даний момент спрощено всі можливі квантові вентилі «X» і один квантовий вентиль «Z» з невикористаних кубітів. Однак, A і B все одно повинні реалізувати по одному квантовому вентилю «Z» за один раз.

Тепер давайте детально розглянемо вентиль CNOT між кубітами $alice_2$ і bob_1 на кроці 2. Він виконує дві функції одночасно. По-перше, як було сказано вище, це частина універсальної телепортації квантових вентилів, яка має з'єднати дві незалежні пари Белла між собою, щоб створити квантову заплутаність між 4 кубітами. Після цього ці два кубіти отримають результат взаємодії вентилів CNOT від кубітів $alice_0$ і bob_3. З іншого боку, цей вентиль виконує операцію CNOT між $alice_2$ і bob_1, яка необхідна для A і B для процедури вимірювання BSM у майбутньому.

Вентиль CNOT, який A і B спільно використовують перед взаємодією з кубітами C, вже виконує необхідну функцію CNOT, яка потрібна A і B. Це квантовий ефект, який неможливо реалізувати класичним способом [12], оскільки кубіти $alice_2$ і bob_1 є частиною більшої замкнутої заплутаної системи. Цей математичний трюк дозволяє нам змусити виконувати процедуру вимірювання BSM перед тим, як A і B точно взаємодіють з кубітами C. Потім, щоб завершити повну процедуру вимірювання BSM для A і B, їм потрібно перемістити квантовий вентиль «H» з кроку 5 на крок 2 і поставити його після вентиля CNOT. Нарешті, A і B виконують процедуру вимірювання BSM вже на кроці 1 зі своїми $alice_2$ і bob_1 перед взаємодією з кубітами C. Але ці кубіти вже є частиною більшого заплутаного стану. На кроці 3, коли кубіти C взаємодіють з кубітами $alice_0$ і bob_3, вони також впливають на кубіти $alice_2$ і bob_1. Тоді, на кроці 5 після вимірювання A і B не потрібно впроваджувати квантові вентилі «X» і «Z», які залежать від результатів вимірювання. Для «фазової» перевірки набір кубітів $alice_0$, $alice_2$, $alice_3$, bob_0, bob_3 дасть різні комбінації бітів після вимірювання, а A з B можуть точно визначити будь-який стан Белла C. Остаточний спрощений варіант квантової схеми визначення стану Белла з використанням квантової телепортації CNOT вентиля наведено на рис. 7.

Спрощення модифікованої оригінальної схеми було досягнуто наступним чином. По-перше, крок 1 і крок 2 об'єднані для підготовки вентилів, які є попередньо спільними заплутаними станами. По-друге, квантовий вентиль «H» перенесено для кубіта $alice_2$ на крок 1. Крім того, класичні біти, які не використовуються, були видалені. Отже, для A і B потрібно підготувати всього 8 кубітів. A і B повинні мати 1 незалежну пару для умови «парності», кубіти $alice_3$ і bob_0, та 1 незалежну пару для умови «фази», кубіти $alice_0$ і bob_3. Крім того, для телепортації квантового вентиля необхідні 2 пари: пара $alice_1$ і $alice_2$ і пара bob_1 і bob_2. Ці пари з'єднані між собою CNOT вентилем між кубітами $alice_2$ і bob_1. Після цього додано квантовий вентиль «H» для кубіта $alice_2$, щоб виконати роботу

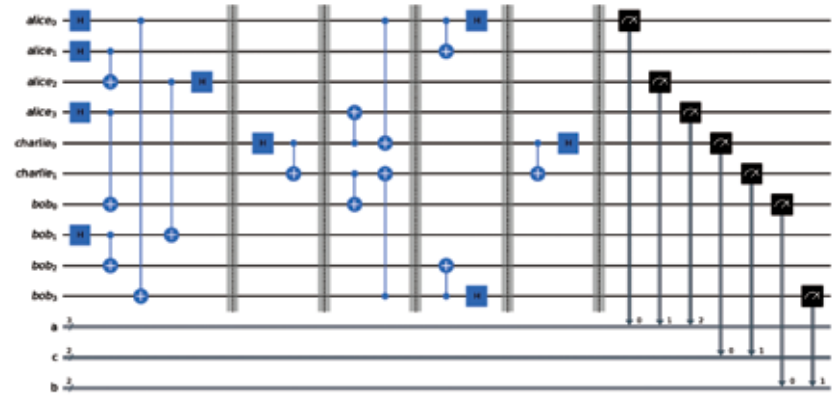

Рис. 7. Спрощена схема визначення стану Белла з використанням квантової телепортації CNOT вентиля

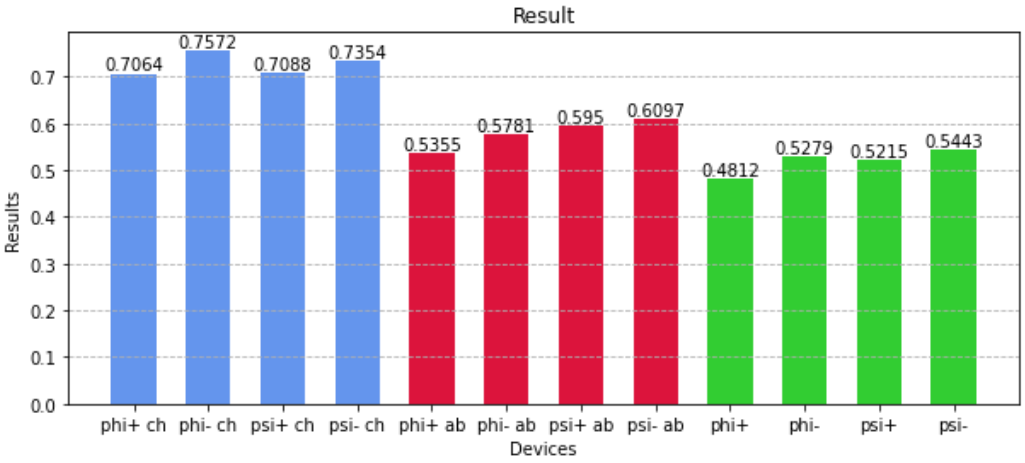

Рис. 8. Результати апробації запропонованої схеми для чотирьох станів Белла

перед процедурою вимірювання BSM для стану «фази». Наведене квантове рішення пройшло успішну апробацію на квантовому комп'ютері IonQ, про що йдеться нижче.

Результати. Запропонована авторами та наведена на рис. 7 спрощена квантова схема дає 100% ймовірність визначення будь-якого стану Белла C. Це було підтверджено при її реалізації на квантовому комп'ютері IonQ. Для цього було зроблено 10 000 знімків для кожного стану Белла C, після чого отримані результати вимірювання представлено на рис. 8. Сині смуги відображають випадок, коли C надсилає деякий стан Белла, а D отримує точно такий же стан, не враховуючи, який стан A та B будуть отримувати, щоб перевірити умову «неруйнівний стан» Белла. Червоні смуги відображають випадок, коли C надсилає деякий стан Белла, а A з B точно визначають цей стан, не враховуючи, який стан отримає D, щоб перевірити умову «визначення стану Белла». Зрештою зелені смуги показують комбінацію двох попередніх випадків, де обидві умови, «неруйнівний стан» і «визначення стану Белла» перевіряються разом. Після цього було розраховано середнє значення для трьох наведених на рис. 8 випадків, щоб визначити середню ймовірність для будь-якого можливого стану Белла (на рис. 9).

Висновки. Запропоноване авторами в роботі квантове схемне рішення показує, як треті сторони можуть розрізняти пари Белла без руйнування оригінального стану для визначення оригінальної інформації від довірених сторін. Запропонована спрощена схема використовує математичний трюк для перевірки «розрізнення станів Белла»

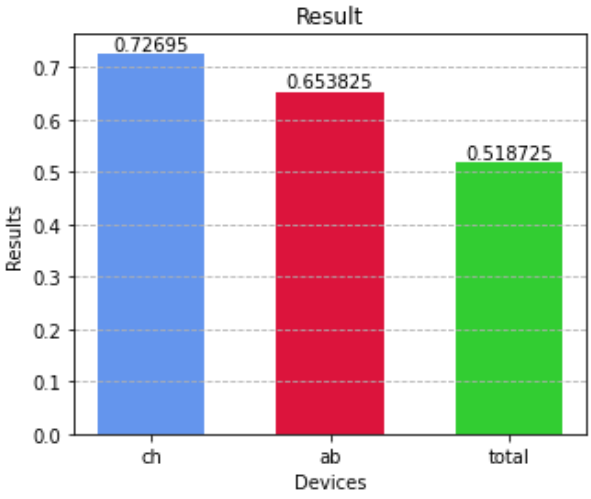

Рис. 9. Середня ймовірність успішної роботи запропонованої схеми на квантовому комп'ютері IonQ

та «неруйнівних» умов, що дає підстави говорити про вдосконалення квантових алгоритмів розподілу ключів.

Однак, ця схема залишається досить громіздкою і використовує багато самих квантових вентилів. Результати її апробації на квантовому комп'ютері IonQ (рис. 9) показали, що ймовірність успішної її роботи становить близько 50%. Однак, класично A та B лише мають ймовірність 25% вгадати стан C, що вдвічі менше отриманого в цій роботі результату (рис. 9).

Крім того, цю схему не можна представити класично, оскільки вона використовує «різницю фаз» між кубітами, що застосовується лише для квантових алгоритмів.

Список літератури:

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.
2. A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.
3. A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?," *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935, doi: 10.1103/PhysRev.47.777.
4. J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Phys. Phys. Fiz.*, vol. 1, no. 3, pp. 195–200, Nov. 1964, doi: 10.1103/PhysicsPhysiqueFizika.1.195.
5. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982, doi: 10.1038/299802a0.
6. M. Gupta and P. K. Panigrahi, "Deterministic Bell State Discrimination," *ArXivquant-Ph0504183*, Apr. 2005, Accessed: Dec. 04, 2021. [Online]. Available: http://arxiv.org/abs/quant-ph/0504183
7. M. Gupta, A. Pathak, R. Srikanth, and P. K. Panigrahi, "Non-destructive Orthonormal State Discrimination," *ArXivquant-Ph0507096*, Jul. 2005, Accessed: Dec. 04, 2021. [Online]. Available: http://arxiv.org/abs/quant-ph/0507096
8. M. Sisodia, A. Shukla, and A. Pathak, "Experimental realization of nondestructive discrimination of Bell states using a five-qubit quantum computer," *Phys. Lett. A*, vol. 381, no. 46, pp. 3860–3874, Dec. 2017, doi: 10.1016/j.physleta.2017.09.050.
9. A. J. Paige, H. Kwon, S. Simsek, C. N. Self, J. Gray, and M. S. Kim, "Quantum Delocalized Interactions," *Phys. Rev. Lett.*, vol. 125, no. 24, p. 240406, Dec. 2020, doi: 10.1103/PhysRevLett.125.240406.
10. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, Mar. 1993, doi: 10.1103/PhysRevLett.70.1895.
11. D. Gottesman and I. L. Chuang, "Quantum Teleportation is a Universal Computational Primitive," *ArXivquant-Ph9908010*, Aug. 1999, doi: 10.1038/46503.
12. https://doi.org/10.1103%2Fphysreva.52.3457

Bilash B.O., Lysenko O.M. ERROR-FREE DEFINITION OF THE QUANTUM BELL STATE IN QUANTUM CRYPTOGRAPHY

The paper discusses one of the most promising methods of modern quantum cryptography – the method of quantum key distribution (QKD) based on pairs of Bell states of quantum entanglement. A generalized quantum scheme is proposed for the detection of the four Bell states by third parties without destroying the original state, which allows third parties to interact individually with each qubit of the Bell pair. At the same time, two tasks were solved at the same time: checking the condition of "determining the state" of Bell, that is, whether it is possible to obtain complete information about the original qubits of the Bell state from trusted parties; on the other hand, checking the "indestructible state" condition, that is, whether it is possible not to destroy the initial Bell state. Since each Bell qubit is sent through a separate path, making the distance between the qubits infinitely large, this precluded the application of the well-known scheme proposed by Gupta et al. Therefore, we used the advantage of entangled states prepared in advance for interaction, which were first considered by Page et al. and developed in this article. For each qubit, the condition of "phase" and "parity" is determined separately, for which separate quantum pairs between third parties are created. Because Bell state qubits can be far apart when transmitting information, third parties cannot directly interact with their qubits, but can exchange classical bits after measuring their qubits. In order to fully obtain information by third parties, the article proposes a new universal teleportation scheme of quantum gates, which was simplified and adapted for the conditions of determining Bell states. This solution provides a 100% probability of determining any Bell state for the ideal case without noise. This scheme is implemented and tested on the IonQ quantum computer.

Key words: *quantum computing, quantum cryptography, quantum cryptoanalysis, Bell state, qubits.*