УДК: 004.056.53

Volodymyr Zinchenko[1], graduate student
ORCID ID: https://orcid.org/0000-0001-6081-4848 ***e-mail:*** zinchenko@outlook.com

Volodymyr Lyfar[2], Doctor of Engineering Sciences, Professor
ORCID ID: https://orcid.org/0000-0002-7860-9663 ***e-mail:*** lifar@snu.edu.ua

[1]Institute of Telecommunications and Global Information Space of the NASU, Kyiv, Ukraine
[2]Volodymyr Dahl East Ukrainian National University, Kyiv, Ukraine

INFORMATION AND MATHEMATICAL MODEL OF QUANTUM COMMUNICATION CHANNEL STATE CONTROL PROCESSES

Abstract. *The most protected and stable communication systems today are quantum channels of information transmission and processing. Thanks to the unique properties of photons as information elements, it becomes possible to monitor and analyze the state of information flows in communication or information transmission channels. Physical attributes such as spin, polarization, radiation frequency, phase synchronization, and the quantum entanglement effect can be tracked and interpreted online to improve the quality and reliability of information in computer systems. In order to effectively use information in support or decision support systems, it is necessary to carefully formalize the processes and indicators of quantum systems for the creation of information processing and transmission, for which information and mathematical models should be created that describe the state of the quantum communication channel (QCC).*

The information model should allow the convolution of the information space. The mathematical model must prove the processes of tracking the states of quantum information and provide a description of the phase state of indicators of the quantum environment. A lock in a closed space with established cause-and-effect relationships is equal to a system of clear logic.

The authors summarize the experience of developing and implementing the method of simulated dynamic modeling of events in an abstract communication channel, which allows formalizing and classifying cause-and-effect relationships of quantum carriers in the analyzed channels. It is proposed to use a unified neural network for the organization of SPPR in quantum-mechanical information transmission systems. Such a network could provide an automatic intelligent system state analysis mode. Such an analysis makes it possible to classify the aggregates of current system parameters to the level of diagnostics of the state of information flows and conclusions based on such diagnostics with the support of decision-making about the quality and reliability of the transmitted information. Such a system, working in OLAP (Online analytical processing) mode, could automatically manage the process of generation and transmission of information, reacting without human intervention to emerging critical errors or attempts at unauthorized system hacking. The observer effect leads to the fact that an attempt to measure the state of a photon inevitably causes an almost instantaneous change in this state. Attempting to parallelize a photon has the same consequences. This cannot be unnoticeable during further authorized acceptance of information. The analyzed quantum communication channel (QCM) consists of a set of technological elements distributed in space. The channel works in its own time, which is formed by clock pulses and creates a flow of information.

Keywords: *information, mathematical model, cryptography, quantum, neural network, information protection, decision support.*

В.Л. Зінченко[1], В.О. Лифар[2]

[1]Інститут телекомунікацій і глобального інформаційного простору НАН України, м. Київ, Україна
[2]Східноукраїнський національний університет імені Володимира Даля, м. Київ, Україна

ІНФОРМАЦІЙНА ТА МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСІВ КОНТРОЛЮ СТАНУ КВАНТОВОГО КАНАЛУ ЗВ'ЯЗКУ

Анотація. *Найбільш захищеними і стійкими системами зв'язку на сьогоднішній день є квантові канали передачі і обробки інформації. Завдяки унікальним властивостям фотонів як інформаційних елементів стає можливим відстежувати і аналізувати стан інформаційних потоків в каналах зв'язку або передачі інформації. Такі фізичні атрибути, як спін, поляризація, частота випромінювання, синхронізація фаз та ефект квантової заплутаності, можна відслідковувати та інтерпретувати в онлайн режимі, щоб покращити якість та достовірність інформації в комп'ютерних системах. Для того щоб ефективно застосовувати інформацію в системах супроводження або підтримки рішень, необхідно ретельно формалізувати процеси та показники квантових систем створення обробки та передачі інформації, для чого слід створити інформаційні та математичні моделі, що описують стан квантового каналу зв'язку (ККЗ).*

Інформаційна модель повинна дозволити згортку інформаційного простору. Математична модель повинна підтвердити процеси відстеження станів квантової інформації та надати опис фазового стану індикаторів квантового середовища. Замкнена система в просторі з усталеними причинно-наслідковими зв'язками рівнозначна системі чіткої логіки.

Автори узагальнюють досвід розробки і впровадження методу імітаційного динамічного моделювання подій в абстрактному каналі зв'язку, що дозволяє формалізувати та класифікувати причинно-наслідкові зв'язки квантових носіїв в аналізованих каналах. Для організації СППР в квантово-механічних системах передачі інформації пропонується використовувати уніфіковану нейронну мережу. Така мережа могла б забезпечити автоматичний інтелектуальний режим аналізу стану системи. Такий аналіз дає можливість класифікації сукупностей поточних параметрів системи до рівня діагностики стану інформаційних потоків і висновків на основі такої діагностики з підтримкою прийняття рішення про якість та надійність переданої інформації. Така система, працюючи в OLAP (Online analytical processing) режимі, могла б автоматично забезпечити управління процесом генерації та передачі інформації, реагуючи без втручання людини на виникаючі критичні помилки або спроби несанкціонованого злому системи. Ефект спостерігача призводить до того, що спроба вимірювання стану фотона неминуче викликає практично миттєву зміну цього стану. Спроба розпаралелювання фотона має ті ж наслідки. Це не може бути непомітним при подальшому санкціонованому прийманні інформації. Канал квантового зв'язку (ККЗ), що аналізується, складається з множини технологічних елементів, розподілених в просторі. Канал працює у власному часі, що формується тактовими імпульсами та створює потік інформації.

Ключові слова: *інформаційна, математична модель, криптографія, квант, нейронна мережа, захист інформації, підтримка рішень.*

https://doi.org/10.32347/2411-4049.2024.3.151-160

Вступ

Авторами запропонована нейронна мережа для діагностики квантового каналу зв'язку – це штучна нейронна мережа, яка здатна виявляти та виправляти помилки, що виникають під час передачі квантової інформації між віддаленими квантовими системами [1–6]. Така мережа може використовуватись для підвищення надійності та безпеки квантового зв'язку, а також для прискорення квантових обчислень.

Одним із прикладів такої нейронної мережі є згорткова нейронна мережа, яка може виявляти патології в квантовому каналі, такі як втрата або деформація фотонів, на основі аналізу спектральних характеристик. Згорткова нейронна мережа складається з кількох шарів, у яких відбувається згортка, підвибірка та класифікація вхідних даних. Згорткова нейронна мережа може бути навчена на великій кількості експериментальних даних, отриманих за різних умов квантового каналу, і потім використовуватися для діагностики нових даних в режимі реального часу.

Постановка задачі

В загальному комплексі заходів щодо забезпечення національної безпеки держави важливе місце займають заходи, пов’язані із безпосереднім захистом інформації від загроз, реалізація яких може завдати особі, суспільству, державі політичні, економічні, фінансові та інші збитки.

Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

1. Здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку. Незважаючи на позитивні зміни в міжнародній обстановці навколо України, діяльність технічних розвідок іноземних держав із здобування інформації продовжується. Проти України безперервно ведеться розвідка багатофункціональними космічними, повітряними, наземними, морськими системами та комплексами технічної розвідки. Провідні країни світу продовжують модернізувати свої розвідувальні служби, вдосконалюють технічну розвідку, нарощують її можливості. Наявні можливості технічних розвідок практично вже сьогодні дають змогу забезпечити безперервне спостереження за всією територією України, і у подальшому, засоби технічної розвідки, зокрема космічної компоненти, будуть мати виключно високі характеристики, які дозволять забезпечити постійне стеження за всією територією держави в реальному масштабі часу.

2. Несанкціонований доступ до інформації, яка обробляється та циркулює в інформаційних та телекомунікаційних системах, а також спеціальний вплив на інформацію з метою її спотворення, руйнування, знищення, порушення нормального функціонування систем обробки інформації. За умови недостатньої номенклатури засобів обробки інформації та програмного забезпечення вітчизняної розробки в інформаційно-телекомунікаційних системах широко використовуються продукти іноземного виробництва, які здебільшого не мають об’єктивних оцінок механізмів захисту, а також створюють передумови впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій. Це зумовило широке

розгортання інформаційно-телекомунікаційних систем, різке збільшення обсягів інформації, що обробляється і зберігається в цих системах, значне збільшення кола користувачів, які мають безпосередній доступ до інформаційних ресурсів, тощо. При цьому, за відсутності конкурентоспроможних вітчизняних зразків, перевага надається інформаційним технологіям та технічним засобам обробки інформації іноземного виробництва, які здебільшого не забезпечують захист інформації, а також створюють передумови неконтрольованого використання спеціальних програмних та апаратних засобів (“закладних пристроїв”). У світі зберігається тенденція поширення масштабів комп’ютерної злочинності, розповсюдження комп’ютерних вірусів, насамперед, з використанням інтернету, істотно зростає небезпека наслідків неправомірних дій, технічних і технологічних помилок та збоїв при застосуванні інформаційно-телекомунікаційних систем, що є особливо актуально в умовах широкого входження вітчизняних інформаційно-телекомунікаційних систем до глобальних. Окремими державами реалізується “концепція інформаційного протиборства”, яка полягає в реалізації заходів щодо спеціального впливу на інформаційну інфраструктуру з метою ураження (знищення) інформаційних ресурсів та руйнування системи управління в сферах оборони, економіки, безпеки, фінансів тощо.

3. Витік інформації з обмеженим доступом технічними каналами внаслідок виникнення побічних електромагнітних випромінювань і наводів, ведення акустичної та оптико-електронної розвідки в безпосередній близькості від об’єкта інформаційної діяльності. В процесі здійснення інформаційної діяльності для зберігання, обробки та передавання інформації, в тому числі й інформації з обмеженим доступом, широко використовуються технічні засоби різного призначення (засоби обчислювальної техніки, оргтехніка, засоби зв’язку, автоматизовані системи тощо). На об’єктах інформаційної діяльності здійснюється обговорення службових питань за різними напрямками діяльності установи, в ході яких може озвучуватися інформація з обмеженим доступом. Проте, окремі фізичні процеси, що відбуваються в технічних засобах та під час обговорення інформації, та інші фактори створюють об’єктивні передумови для появи технічних каналів витоку інформації, що зумовлює необхідність реалізації заходів зі створення комплексів (систем) технічного захисту інформації, спрямованих на запобігання витоку інформації цими каналами.

При моделюванні використовуються квантові коди, що виправляють помилки. При передачі інформації по каналу з шумом, а також при виконанні квантових операцій бажано використовувати код, який був би стійкий щодо помилок. У класичному випадку принципова можливість такого кодування при швидкостях передачі, менших за пропускну здатність, випливає з теореми Шеннона. Однак ця теорема не дає конструктивного способу побудови перешкодостійкого коду, і практичному вирішенню цієї проблеми присвячена значна частина досліджень з теорії інформації, що становить теорію кодування.

Найпряміший спосіб застрахуватися від помилок полягає у повторенні повідомлень (що, звичайно, знижує швидкість передачі). Нехай в алфавіті є всього два символи 0, 1. Тоді припустимо, що ймовірність зміни одного біта в процесі передачі дорівнює малій величині p, так що ймовірність зміни двох бітів p2 зневажливо мала. Розглянемо код $0 \rightarrow 00$, $1 \rightarrow 11$. Хоча цей код і дозволяє виявити та виправити деякі помилки, він має істотний недолік:

наприклад, у ситуації однієї помилки у другому чи першому біті 00 → 01, 11 → 01 ми можемо сказати, яке повідомлення було закодовано. Але цього недоліку можна позбутися, якщо додати ще один розряд: 0 → 000, 1 → 111. Такий код буде вже на заваді стійким по відношенню до помилки в будь-якому одному біті, в тому сенсі, що зіпсовані слова, що виходять з 000 і 111, ніколи не збігаються і тому безпомилково помітні [7–12].

У квантовій статистиці безпомилкова помітність чистих станів (а ми тут матимемо справу тільки з ними) рівносильна ортогональності векторів станів. Прямолінійне узагальнення класичного рецепту повторення повідомлень на квантовий випадок наштовхується на труднощі – квантову інформацію неможливо розмножити. По суті квантової інформації, під час передачі через канал з помилками безпомилково повинні прийматися як базисні стани, та й усілякі їх суперпозиції $|\psi\rangle$. Таким чином, прямолінійне узагальнення коду повторення $\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ є нездійсненним. На перший погляд, завдання здається нерозв'язним, проте у роботах Шора і Стіна незалежно були побудовані перші приклади квантових кодів, які виправляють помилки [12–17].

Необхідно розробити інформаційну та математичну моделі для згортки та замкнення простору обчислювань в області визначення та області застосування моделей, що імітують реальні канали квантового зв’язку.

Вирішення поставленої задачі

Авторами узагальнена математична модель процесів контролю стану системи квантової передачі інформації та алгоритмів підтримки рішень, що може бути представлена кортежем:

$$GIQ = \langle PK, R, Qb, F(S), Kk, DSS \rangle, \quad (1)$$

де $Pk = \{ pk_j \}$ – множина показників квантового каналу зв’язку;

R – множина регістрів каналу зв'язку по розрядах;

Qb – множина інформаційних елементів Q бітів, які формують стан фотонного середовища каналу зв'язку;

$F(S) = \{ f(s_i) \}$ – функція розробки прийняття рішення, як повне сюр'єктивне відображення множини симптомів S на множину рішень DSS;

Kk – множина показників квантового каналу зв'язку, що відповідає формуванню стану порозрядних елементів;

DSS – множина елементарних рішень, що формують алгоритми дій в системі підтримки прийняття рішень.

Передбачається, що відомі детерміновані показники фізичних процесів, які можуть виникати в *i*-й підсистемі для *j*-х станів, що відображає вектор симптомів на вектор подій:

$$fe_{ij} : \vec{S}_{ij} \rightarrow \vec{\Phi}_{ij}, j = 1..J, \quad (2)$$

де j – набір елементарних подій, що призводять до відмов в каналі, $\vec{S}_{ij}$ – вектор параметрів, що відповідає поточному стану *i*-ї підсистеми; $\vec{\Phi}_{ij}$ – вектор фазових змінних квантових процесів, які можуть виникнути в *i*-й підсистемі.

Розглядається узагальнена інформаційна модель нештатної ситуації в ККЗ для аналізу і передбачення наслідків відмов.

Для розробки надійної системи класифікації стану лінії квантового передавання інформації пропонується використовувати гібридні методи аналізу та захисту від небезпеки каналів зв'язку, які, з одного боку, забезпечують надійність діагностування станів системи, а з іншого – надають можливість активного застосування математичного кодування сигналів для збільшення надійності каналів зв'язку до прийнятного рівня. На основі досвіду використання різних кодів автор рекомендує описаний нижче модифікований алгоритм протоколу BB84 та інші його різновиди.

Ідея полягає в наступному: є два віддалених один від одного учасники, A та B, які потребують спільний бінарний ключ, тобто послідовність $\kappa = (\kappa_1, \ldots, \kappa_m)$ довжини m. Цей ключ учасники бажають використовувати для кодування та декодування своїх повідомлень, які також є бінарними послідовностями довжини m, за допомогою операції XOR посимвольно: $y_k = x_k \oplus \kappa_k$, $x_k = y_k \oplus \kappa_k$. Тут $x = (x_1, \ldots, x_m)$ – повідомлення, яке кодується, а $y = (y_1, \ldots, y_m)$ – закодоване повідомлення, яке A відправляє B для подальшого декодування. Цей метод кодування/декодування відомий як шифр Вернама.

Протоколи розподілу секретного ключа.

Оскільки ключ має бути секретним, важливою проблемою є знаходження способу його передачі (розподілу) обом учасникам, за якого ключ не може бути перехоплений або пошкоджений. Квантова криптографія пропонує такі способи (протоколи), надійність яких може бути в принципі як завгодно висока і забезпечується закономірностями квантової інформатики, такими як неможливість клонування квантового стану і додатковість між квантовим вимірюванням і збуренням стану.

Усі викладені нижче протоколи використовують той факт, що стани $|0\rangle$, $|1\rangle$ збурюються під час вимірювання в базисі $\{|+\rangle, |-\rangle\}$, точніше, з імовірністю 1/2 переходять у стани $|+\rangle$ або $|-\rangle$, і навпаки, стани $|+\rangle$, $|-\rangle$ під час вимірювання в базисі $\{|0\rangle, |1\rangle\}$ переходять у стани цього базису.

Протокол BB84, запропонований Беннетом і Брассаром, можна модифікувати в наступні кроки:

1. Учасник A створює дві випадкові двійкові послідовності $a = (a_1,\ldots,a_N)$, $b = (b_1,\ldots,b_N)$ довжиною $N = (4+\delta)n$, $n \gg 1$, також враховуючи, що кожен біт a_k, b_l незалежний і має розподіл $\{\frac{1}{2}, \frac{1}{2}\}$.

2. Учасник A створює чистий квантовий стан з вектором

$$|\phi\rangle = \otimes_{k=1}^{N} |\phi_{a_k b_k}\rangle,$$

$$|\phi_{00}\rangle = |0\rangle, \qquad |\phi_{10}\rangle = |1\rangle,$$

$$|\phi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |\phi_{01}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\cdot$$

3. Учасник A надсилає цей стан учаснику B відкритим квантовим каналом. Якщо канал ідеальний (шум або стороннє втручання відсутні), то B отримує стан $|\psi\rangle\langle\psi|$, в іншому разі – збурений стан $E(|\psi\rangle\langle\psi|)$, де E позначає дію каналу.

Учасник B генерує випадкову послідовність $b' = (b_1', \ldots, b_N')$ і на *k*-му кроці здійснює вимірювання в базисі $\{|0\rangle, |1\rangle\}$, якщо $b_k' = 0$, або в базисі $\{|+\rangle, |-\rangle\}$, якщо $b_k' = 1$. Результати його вимірювань утворюють двійкову послідовність $a' = (a_1', \ldots, a_N')$.

4. Учасник A надсилає послідовність b учаснику B через відкритий класичний канал. B порівнює b з b′ і повідомляє A номери бітів, які співпадають ($b_k = b_k'$).

Якщо канал ідеальний, то для цих бітів з імовірністю 1 виконується $a_k = a_k'$, бо вимірювання проводили в базисі, що містить надісланий стан. З великою ймовірністю кількість таких бітів майже дорівнює половині від N, що дорівнює $(2 + \delta/2)n \geq 2n$. Якщо кількість співпадаючих бітів a і a′ значно відрізняється від 2n, це означає можливість стороннього втручання у квантовий канал передачі. Тому учасники A і B припиняють передачу і намагаються усунути можливість втручання.

5. A і B виконують тести, щоб визначити величину втручань через можливий шум або підслуховування. Для цього A випадково обирає n бітів відфільтрованого ключа і передає їхні значення (разом з номерами) учаснику B через відкритий канал. Імовірність отримати $\leq \nu n$ помилок у цих n контрольних бітах і при цьому $\geq (\nu+\varepsilon)n$ помилок у решті бітів має порядок $\exp[O(\varepsilon^2 n)]$. Тому за великих n можна вважати, що частка розбіжностей у цих секретних бітах, що залишилися, практично дорівнює ν. Якщо A і B виявляють, що ν перевершує деяке порогове значення ν_t, то вони вирішують, що було втручання, і також припиняють цей раунд протоколу. Величина νt залежить від того, що відомо про можливості перехоплювача E. У літературі наводять значення $\nu_t = 0.11 \div 0.25$, залежно від виду атак перехоплювача і використовуваних засобів протидії. Докладніше про це див. у [3].

6. Якщо встановлено, що $\nu < \nu_t$, то A і B здійснюють "узгодження інформації", щоб усунути неспівпадіння бітів, і "підвищення конфіденційності" залишковими $\approx$ n бітами, щоб знищити інформацію, яку міг перехопити E під час попередніх відкритих операцій. При цьому дуже корисною є верхня квантова оцінка кількості інформації перехоплювача E. Останні операції відносяться до класичної інформатики. В результаті A і B отримують m×n бітів спільного секретного ключа.

Покажемо, що у разі малих δ

$$P\left\{2n \leq (\#k{:}b_k = b_k') \leq (2+\delta)n\right\} \geq 1 - 2\exp\left[-\frac{1}{8}n(\delta^2 + o(\delta^2))\right]. \qquad (3.1)$$

Вводячи біт розбіжності $\nu_k = b_k \oplus b_k'$, маємо $P\{\nu_k = 0\} = P\{\nu_k = 1\} = \frac{1}{2}$, $M\nu_k = \frac{1}{2}$. Ймовірність, що нас цікавить, дорівнює (N = (4 + δ)n)

$$P\left\{2n \leq \sum_{k=1}^{N} \nu_k \leq (2+\delta)n\right\} = 1 - 2P\left\{\sum_{k=1}^{N} (\nu_k < 2n\right\},$$

унаслідок симетрії розподілу суми щодо її математичного очікування N/2 = (2 + δ/2)n, у такому разі

$$P\left\{\sum_{k=1}^{N} v_k < 2n\right\} = P\left\{\frac{1}{N}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right) < -\varepsilon\right\},$$

де $\varepsilon = \frac{1}{2} - \frac{2n}{(4+\delta)n} = \frac{1}{8}(\delta + o(\delta))$. Зауважимо, що при використанні нерівності Чебишева, під час доведення закону великих чисел, випливає

$$P\left\{\left|\frac{1}{N}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right)\right| > \varepsilon\right\} \le \frac{Dv_k}{N\varepsilon^2} = \frac{1}{4N\varepsilon^2} \to 0$$

при N → ∞. Експоненціальна оцінка (3.2), набагато точніша за експоненціальну, що випливає з нерівності Чернова:

$$P\left\{\frac{1}{N}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right) \le -\varepsilon\right\} = P\left\{\frac{1}{N}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right) \ge \varepsilon\right\} \le \exp\left[-2N\left(\varepsilon^2 + \left(\varepsilon^2\right)\right)\right]. \quad (3.2)$$

Це випливає з наступного. Нехай s > 0, тоді

$$P\left\{\frac{1}{N}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right) \ge \varepsilon\right\} = P\left\{e^{s}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right) \ge e^{sN\varepsilon}\right\} \le e^{-sN\varepsilon} M e^{s}\sum_{k=1}^{N}\left(v_k - \frac{1}{2}\right)$$

$$= e^{-sN\varepsilon}\left[M e^{s\left(v_k - \frac{1}{2}\right)}\right]^N = e^{-sN\varepsilon}\left[\cosh\frac{s}{2}\right]^N = e^{-N\left(s\varepsilon - \ln\cosh\frac{s}{2}\right)}.$$

При малих значеннях s

$$\ln\cosh\frac{s}{2} = \frac{s^2}{8} + o(s^2).$$

З іншого боку,

$$\max\left(s\varepsilon - \frac{s^2}{8}\right) = 2\varepsilon^2, s \ge 0,$$

до того ж максимум досягається для s = 4ε. Звідси отримуємо (3.2), а враховуючи, що N = (4 + δ)n, маємо (3.1).

Протокол B92 (додаткові дані).

1. Учасник A генерує випадкову двійкову послідовність a = (a1, . . . , aN) і на кожному кроці k створює чистий стан з вектором $|\psi_0\rangle = |0\rangle$, якщо ak = 0, або $|\psi_1\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, якщо $a_k = 1$.

2. Учасник A відправляє стан, задаючи вектором $|\phi\rangle = \otimes_{k=1}^{N} |\phi_{a_k}\rangle$, учаснику B по відкритому квантовому каналу.

Учасник B генерує випадкову послідовність a'=(a_1',…,a_N'), у *k*-тому кроці виконує вимірювання у базисі {|0⟩|1⟩}, якщо $a_k' = 0$, або у базисі {|+⟩|-⟩}, $a_k' = 1$. Східний плюс кодується як 0, мінус як 1. Таким чином, результат вимірювання B утворює двійкову послідовність b = (b_1,…,b_N). Слід також зазначити, що ak = a_k', тоді $b_k = 0$, тому з $b_k = 1 \Rightarrow a_k \neq a_k'$, тобто $a_k = 1 - a_k'$.

3. Учасник B відправляє послідовність b учаснику A по відкритому класичному каналу. A (відповідно B) залишає тільки ті біти послідовності a (відповідно a'), для яких $b_k = 1$. Отримані таким чином таємні біти $a_k = 1\text{-}a_k'$ складають відфільтрований ключ.

4. Наступні кроки аналогічні відповідним крокам протоколу BB84.

Протокол E91.

Учасники A і B отримують "половинки" зчепленого стану

$$\left|\phi\right\rangle = \otimes_{k=1}^{N} \left|\phi_{a_k}\right\rangle$$

де: $\left|\phi_k\right\rangle = \frac{1}{2}\left(\left|100\right\rangle + \left|11\right\rangle\right) = \frac{1}{\sqrt{2}}\left(\left|++\right\rangle + \left|--\right\rangle\right),$ (3.3)

де перший q-біт надсилається учаснику A, а другий – B.

Учасник A генерує випадкову двійкову послідовність $a = (a_1, \ldots, a_N)$. На *k*-му кроці A проводить вимірювання в базисі $\{|0\rangle, |1\rangle$, якщо $a_k = 0$, або в базисі $\{|+\rangle, |-\rangle\}$, якщо $a_k = 1$, та отримує результати $a' = (a_1', \ldots, a_N')$. Відповідно B генерує послідовність $b = (b_1, \ldots, b_N)$, вимірює в базисі, обраному за b_k, і отримує результати $b' = (b_1', \ldots, b_N')$.

З рівності (3.3) випливає, що якщо на *k*-му кроці A і B проводять вимірювання в однакових базисах: $\{|0\rangle, |1\rangle\}$ або $\{|+\rangle, |-\rangle\}$, то вони отримують співпадаючі результати, $P\{a_k' = b_k'\} = 1$.

Використовуючи відкритий класичний канал, A і B порівнюють a і b і залишають у відфільтрованому ключі тільки ті біти a′ (відповідно b′), для яких $a_k = b_k$, тобто A і B використовували для *k*-го вимірювання однакові базиси. У цьому протоколі біти просіяного ключа $a_k' = b_k'$ не просто відбирають, але створюють під час вимірювань.

Описані вище протоколи реалізовано в експерименті; більше того, для перших двох створено комерційні зразки обладнання. Доведення їхньої стійкості є непростим завданням, яке вимагає залучення всього інструментарію квантової теорії інформації.

Висновки

Гібридне використання інтелектуального аналізу станів ККЗ на основі нейронної мережі та криптографічних протоколів при створенні стійких ключів безпечного шифрування дає прийнятний результат по захисту квантових каналів від кіберзламів.

Інформаційна та математична модель, що розроблена авторами, дає згортку інформаційного простору до рівня, який можна обчислити. Кортеж інформаційної моделі містить замкнуті математичні вирази та відображення, що є гладкими та не мають розривів і, таким чином, можуть бути похідними, що необхідно для розрахунків ваг зв’язків в нейронній мережі.

REFERENCES

1. Huang, D., Chen, Z., Guo, Y., & Lee, M. (2007). Quantum Secure Direct Communication Based on Chaos with Authentication. *Journal of the Physical Society of Japan*, 76(12), 124001.
2. TLS (Channel SSP) changes in Windows 10 and Windows Server. (2018). Microsoft. Docs. Retrieved May 09, 2020 from https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windowsserver
3. Valiev, K.A., & Kokin, A.A. (2004). Kvantovie kompyuteri: nadezhdi i realnost [Quantum Computers: Hopes and Reality] (2nd ed.). Moscow: IKI [in Russian].
4. Hiai, F. & Petz, D. (1991). The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.* 143, 99.
5. A Quantum information processing and quantum error correction: An engineering approach. (2012). Elsevier. Retrieved from https://doi.org/10.1016/c2010-0-66917-3
6. Information and Computation: Classical and Quantum Aspects. (2001). Reviews of Modern Physics to apperar. Retrieved from https://arxiv.org/pdf/quant-ph/0112105
7. Shifrin, T., & Adams, M. (n.d.). Linear Algebra and Geometry. W. H. Freeman.
8. von Neumann, J. (1955). Mathematical Foundations of Quantum Mechanics (1st Edition). Princeton University Press.
9. Nielsen, M., & Chuang, I. (2011). Quantum Computation and Quantum Information (10th Anniversary Edition). Cambridge University Press.
10. Faddeev, L.D., & IĂkubovskiĭ, O.A. (2009). Lectures on Quantum Mechanics for Mathematics Students. American Mathematical Soc.
11. Sands, M., & Feynman R.P. (2011). The Feynman Lectures on Physics, Vol. III. Basic Books; New Millennium ed. edition.
12. Khatri, S., & Wilde, M. M. (2020). Principles of Quantum Communication Theory: A Modern Approach. arXiv:2011.04672.
13. Giroti, I., & Malhotra, M. (2022). Quantum Cryptography: A Pathway to Secure Communication. In 6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (2022, №6, p. 279).
14. Regula, B., Lami, L., & Wilde, M.M. (2022). Postselected quantum hypothesis testing. arXiv:2209.10550.
15. Bierbrauer, J. (2016). Introduction to Coding Theory (2nd Edition). New York.
16. Lami, L. & Shirokov, M.E. (2021). Attainability and lower semi-continuity of the relative entropy of entanglement, and variations on the theme. arXiv:2105.08091.
17. Watrous, J. (n.d.). The theory of quantum information. Retrieved from http://cs.uwaterloo.ca/~watrous/TQI/TQI.pdf

Стаття надійшла до редакції 07.05.2024 і прийнята до друку після рецензування 09.08.2024

The article was received 07.05.2024 and was accepted after revision 09.08.2024

Зінченко Володимир Леонідович
аспірант, Інститут телекомунікацій і глобального інформаційного простору НАН України
Адреса робоча: 03186 Україна, м. Київ, Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0000-0001-6081-4848 ***e-mail:*** zinchenko@outlook.com

Лифар Володимир Олексійович
д.т.н., професор, Східноукраїнський національний університет імені Володимира Даля
Адреса робоча: вул. Іоанна Павла II, 17, м. Київ, 01042, Україна
ORCID ID: https://orcid.org/0000-0002-7860-9663 ***e-mail:*** lifar@snu.edu.ua