УДК 003.26:621.39+530.145

Василіу Є.В., Мамедов Р.С.
Василиу Е.В., Мамедов Р.С.
Vasiliu E.V., Mamedov R.S.

АНАЛІЗ АТАКИ ПАСИВНОГО ПЕРЕХОПЛЕННЯ НА ПІНГ-ПОНГ ПРОТОКОЛ З ЧОТИРИКУБІТНИМИ КЛАСТЕРНИМИ СТАНАМИ ЯК ЕЛЕМЕНТ СИНТЕЗУ КВАНТОВОЇ СИСТЕМИ БЕЗПЕЧНОГО ЗВ'ЯЗКУ

АНАЛИЗ АТАКИ ПАССИВНОГО ПЕРЕХВАТА НА ПИНГ-ПОНГ ПРОТОКОЛ С ЧЕТЫРЕХКУБИТНЫМИ КЛАСТЕРНЫМИ СОСТОЯНИЯМИ КАК ЭЛЕМЕНТ СИНТЕЗА КВАНТОВОЙ СИСТЕМЫ БЕЗОПАСНОЙ СВЯЗИ

ANALYSIS OF EAVESDROPPING ATTACK ON THE PING-PONG PROTOCOL WITH FOUR-QUBIT CLUSTER STATES AS AN ELEMENT OF SYNTHESIS OF SECURE COMMUNICATION QUANTUM SYSTEM

Анотація. *На основі методів квантової теорії інформації проаналізована атака пасивного перехоплення на пінг-понг протокол із чотирикубітними кластерними станами. Показано, що при використанні легітимними користувачами в режимі контролю підслуховування двох вимірювальних базисів протокол має асимптотичну стійкість до такої атаки, аналогічно пінг-понг протоколу із багатокубітними ГХЦ-станами. Показано також, що протокол із кластерними станами має ряд переваг перед аналогічним протоколом із ГХЦ-станами, як за критерієм стійкості до атаки пасивного перехоплення, так і за критерієм стійкості до природних завад у квантовому каналі зв'язку.*

Аннотация. *На основе методов квантовой теории информации проанализирована атака пассивного перехвата на пинг-понг протокол с четырехкубитными кластерными состояниями. Показано, что при использовании легитимными пользователями в режиме контроля подслушивания двух измерительных базисов протокол обладает асимптотической стойкостью к такой атаке, аналогично пинг-понг протоколу с многокубитными ГХЦ-состояниями. Показано также, что протокол с кластерными состояниями имеет ряд преимуществ перед аналогичным протоколом с ГХЦ-состояниями, как по критерию стойкости к атаке пассивного перехвата, так и по критерию устойчивости к естественным помехам в квантовом канале связи.*

Summary. *The eavesdropping attack on the ping-pong protocol with four-qubit cluster states is analyzed using the methods of quantum information theory. It is shown, that the protocol is asymptotic secure against such attack using two measuring bases by legitimate users in a control mode, similarly to ping-pong protocol with many-qubit GHZ-states. It is also shown, that the protocol with cluster states has several advantages over the similar protocol with GHZ-states, as by criterion of security to eavesdropping attack, and by criterion of resistance to natural noise in a quantum communication channel.*

Методи квантової криптографії швидко розвиваються в останні два десятиріччя й пропонують нові підходи до побудови захищених систем конфіденційного зв'язку. Робота таких систем, які ґрунтуються на протоколах квантової криптографії, потребує використання не тільки самих квантово-криптографічних протоколів, а і додаткових засобів класичної криптографії та кодування інформації для забезпечення високого рівня ефективності всієї системи та її стійкості як до атак зловмисника, так і до природних завад у квантових каналах зв'язку. Так, передавання інформації квантовим каналом є тільки одним з елементів стека протоколів квантового розподілення секретних ключів, інші елементи стека – це процедури виправлення помилок та підсилення секретності, які ґрунтуються на методах як квантової, так і класичної теорії інформації [1].

Аналогічно системи конфіденційного зв'язку, які ґрунтуються на квантових протоколах прямого безпечного зв'язку, як правило, не можуть бути побудовані тільки на цих протоколах, а потребують додаткових засобів підсилення секретності, завадостійкого кодування тощо [2]. Тому постає проблема синтезу всіх цих елементів в єдину систему безпечного зв'язку, для чого потрібно розв'язати цілий ряд окремих завдань. Так, першим етапом такого синтезу є розробка нового квантового протоколу (або вдосконалення за якимись параметрами вже запропонованого), тобто розробка схеми квантового кодування інформації та схеми контролю перехоплення інформації в квантовому каналі. Далі необхідно обчислити рівень стійкість протоколу до можливих видів атак, зокрема, атаки пасивного перехоплення, тобто обчислити кількість інформації, яка може бути перехоплена зловмисником у залежності від параметрів протоколу. Ці два етапи виконуються з

використанням методів квантової механіки та квантової теорії інформації. Зокрема, для розрахунків широко використовується алгебричний формалізм опису квантових станів, введений в квантову механіку П. Діраком (позначення Дірака) [1, 3]. В даній роботі розрахунки виконані з використанням формалізму Дірака.

Наступний етап синтезу квантової системи конфіденційного зв'язку, що ґрунтується на отриманих результатах аналізу стійкості протоколу, – це розробка процедур підсилення стійкості, якщо такі процедури можливі для даного протоколу. Також необхідно вибрати ефективний завадостійкий код, квантовий або класичний, з урахуванням особливостей передавання інформації в даному протоколі [2].

Одним з простих, але ефективних протоколів квантового безпечного зв'язку є так званий пінг-понг протокол, для якого вже розроблено декілька варіантів [4…10]. Один з таких варіантів – протокол з чотирикубітними кластерними (Ω) станами, запропонований в роботі [10], який має переваги над аналогічним протоколом зі станами Грінбергера–Хорна–Цайлінгера (ГХЦ) [7]. Однак атака пасивного перехоплення (підслуховування) на цей протокол проаналізована не була. Метою цієї роботи є аналіз такої атаки, що є необхідним елементом синтезу квантової системи конфіденційного зв'язку, яка ґрунтується на відповідному пінг-понг протоколі.

1. Пінг-понг протокол з чотирикубітними кластерними станами

Наведемо короткий опис цього протоколу.

Шістнадцять ортонормованих переплутаних чотирикубітних Ω-станів мають вид [10]:

$$|\Omega_1\rangle = \big(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle\big)/2; \quad |\Omega_2\rangle = \big(|0000\rangle + |0110\rangle - |1001\rangle + |1111\rangle\big)/2;$$
$$|\Omega_3\rangle = \big(|0000\rangle - |0110\rangle + |1001\rangle + |1111\rangle\big)/2; \quad |\Omega_4\rangle = \big(|0000\rangle - |0110\rangle - |1001\rangle - |1111\rangle\big)/2;$$
$$|\Omega_5\rangle = \big(|0001\rangle + |0111\rangle + |1000\rangle - |1110\rangle\big)/2; \quad |\Omega_6\rangle = \big(|0001\rangle + |0111\rangle - |1000\rangle + |1110\rangle\big)/2;$$
$$|\Omega_7\rangle = \big(|0001\rangle - |0111\rangle + |1000\rangle + |1110\rangle\big)/2; \quad |\Omega_8\rangle = \big(|0001\rangle - |0111\rangle - |1000\rangle - |1110\rangle\big)/2;$$
$$|\Omega_9\rangle = \big(|0010\rangle + |0100\rangle + |1011\rangle - |1101\rangle\big)/2; \quad |\Omega_{10}\rangle = \big(|0010\rangle + |0100\rangle - |1011\rangle + |1101\rangle\big)/2;$$
$$|\Omega_{11}\rangle = \big(|0010\rangle - |0100\rangle + |1011\rangle + |1101\rangle\big)/2; \quad |\Omega_{12}\rangle = \big(|0010\rangle - |0100\rangle - |1011\rangle - |1101\rangle\big)/2;$$
$$|\Omega_{13}\rangle = \big(|0011\rangle + |0101\rangle + |1010\rangle - |1100\rangle\big)/2; \quad |\Omega_{14}\rangle = \big(|0011\rangle + |0101\rangle - |1010\rangle + |1100\rangle\big)/2;$$
$$|\Omega_{15}\rangle = \big(|0011\rangle - |0101\rangle + |1010\rangle + |1100\rangle\big)/2; \quad |\Omega_{16}\rangle = \big(|0011\rangle - |0101\rangle - |1010\rangle - |1100\rangle\big)/2, \quad (1)$$

де $|0\rangle$ та $|1\rangle$ – базисні стани одного кубіта, які утворюють так званий *z*-базис (базис B_z) і відповідають вертикальній й горизонтальній поляризації фотона.

Оскільки шістнадцять Ω-станів нормовані й взаємно ортогональні, то вони утворюють базис у гільбертовому просторі чотирьох кубітів і відповідно можуть бути точно відрізнені один від одного вимірюванням в цьому базисі.

Боб (приймаюча сторона) приготовляє стан $|\Omega_1\rangle$. Він залишає в себе перші два кубіти («домашні кубіти») й посилає третій і четвертий («передавані кубіти») Алісі (передавальна сторона) по квантовому каналу зв'язку. Аліса випадково перемикається між режимом передачі повідомлення й режимом контролю підслуховування.

У режимі передачі повідомлення (рис. 1) Аліса виконує унітарну кодувальну операцію U_{ijkl} (i, j, k, l = 0, 1) над двома передаваними кубітами і посилає їх назад Бобові.

Кодувальні операції Аліси над третім та четвертим кубітами, які перетворюють стан $|\Omega_1\rangle$ в стани $|\Omega_1\rangle$,…, $|\Omega_{16}\rangle$ відповідно, мають вид:

$$U_{0000} = I \otimes I; \; U_{0001} = I \otimes \sigma_z; \; U_{0010} = \sigma_z \otimes I; \; U_{0011} = \sigma_z \otimes \sigma_z; \; U_{0100} = I \otimes \sigma_x; \; U_{0101} = I \otimes i\sigma_y;$$
$$U_{0110} = \sigma_z \otimes \sigma_x; \; U_{0111} = \sigma_z \otimes i\sigma_y; \; U_{1000} = \sigma_x \otimes I; \; U_{1001} = \sigma_x \otimes \sigma_z; \; U_{1010} = i\sigma_y \otimes I;$$
$$U_{1011} = i\sigma_y \otimes \sigma_z; \; U_{1100} = \sigma_x \otimes \sigma_x; \; U_{1101} = \sigma_x \otimes i\sigma_y; \; U_{1110} = i\sigma_y \otimes \sigma_x; \; U_{1111} = i\sigma_y \otimes i\sigma_y, \quad (2)$$

і відповідають наступним чотирибітовим рядкам: «0000», «0001», «0010», «0011», «0100», «0101», «0110», … В (2) $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ – тотожний оператор; $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ та $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ – оператори Паулі [1, 3].

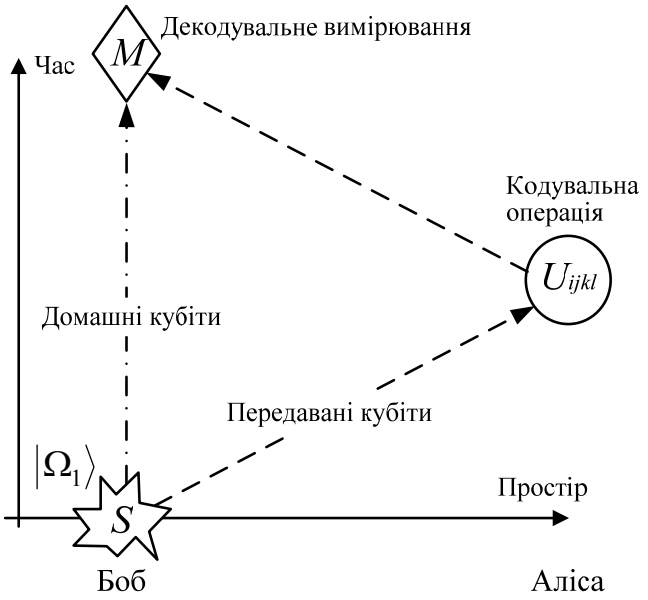

Рисунок 1 – Режим передавання повідомлення, *S* – джерело переплутаних станів $|\Omega_1\rangle$

Одержавши два кубіти назад від Аліси, Боб виконує вимірювання над всіма чотирма кубітами в Ω-базисі й, тим самим, напевне визначає чотирибітовий рядок, який вона послала (див. рис. 1).

У режимі контролю підслуховування (рис. 2) Аліса випадково вибирає один із двох вимірювальних базисів: $B_z = \{|0\rangle\langle 0|; |1\rangle\langle 1|\}$ або $B_x = \{|+\rangle\langle +|; |-\rangle\langle -|\}$, де $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ та $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, й виконує вимірювання станів третього й четвертого кубітів в обраному базисі, а потім повідомляє Бобові за звичайним відкритим, але автентифікованим каналом вибраний нею базис та отримані результати вимірювань. Автентифікація всіх повідомлень, що передаються у звичайному каналі, необхідна для запобігання атаки «людина посередині». Потім Боб у тому ж базисі, що й Аліса, вимірює стани першого й другого кубітів.

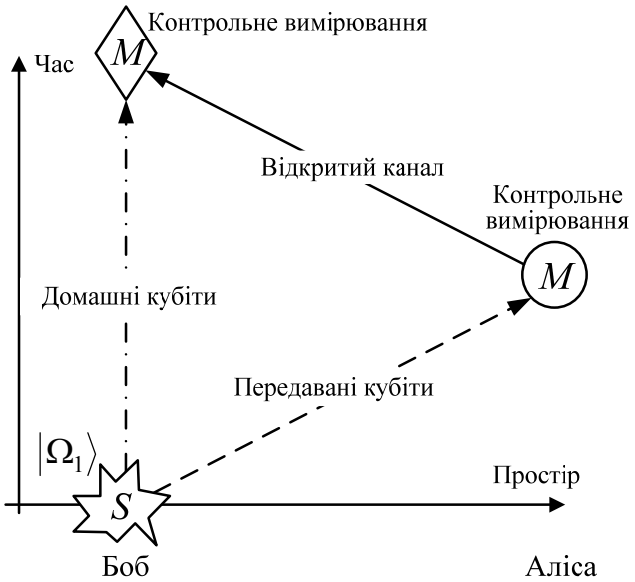

Рисунок 2 – Режим контролю підслуховування

Результати вимірювань Аліси й Боба за описаною схемою наведені у табл. 1 [10]. Аліса, вимірюючи стани третього та четвертого кубітів у базисі B_z, одержує «0» або «1» з однаковою ймовірністю $1/2$, і аналогічно одержує з імовірністю $1/2$ «+» або «–» при вимірюванні в базисі B_x. Боб повинен одержати результати своїх вимірювань з імовірністю 1 як для першого, так і для другого кубітів.

Таблиця 1 – Схема й результати вимірювань для контролю підслуховування

Результати Аліси		Стан після вимірювань Аліси	Результати Боба	
кубіт 3	кубіт 4		кубіт 1	кубіт 2
Базис $\|B_z\rangle$				
0	0	$\|0000\rangle$	0	0
	1	$\|1001\rangle$	1	0
1	0	$\|0110\rangle$	0	1
	1	$\|1111\rangle$	1	1
Базис $\|B_x\rangle$				
+	+	$\|++++\rangle$	+	+
	–	$\|-++-\rangle$	–	+
–	+	$\|+--+\rangle$	+	–
	–	$\|----\rangle$	–	–

Наведені в табл. 1 результати Боб буде отримувати з ймовірністю, рівною одиниці, тільки при використанні ідеального квантового каналу та при відсутності підслуховування. Тому для ідеального каналу у випадку розбіжності результатів вимірювань Боба з очікуваними він негайно сповіщає про це Алісі за звичайним каналом й протокол переривається. У реальному квантовому каналі із шумом Аліса й Боб повинні будуть виконати деяку кількість раундів контролю підслуховування, щоб оцінити рівень помилок при вимірюваннях Боба й порівняти його з очікуваним граничним рівнем природних помилок у каналі. Перевищення цього граничного рівня приписується атаці зловмисника (Єві) й протокол переривається.

2. Аналіз атаки пасивного перехоплення на пінг-понг протокол з чотирикубітними кластерними станами. Схема атаки пасивного перехоплення однакова для всіх варіантів пінг-понг протоколу і полягає в наступному. Єва повинна спочатку виконати атакуючу операцію $\widehat{E}$, переплутуючи свою допоміжну квантову систему (пробу) з передаваними кубітами на шляху Боб $\rightarrow$ Аліса, а після виконання Алісою однієї з кодувальних операцій (2), виконати вимірювання над складеною системою "передавані кубіти – проба" (рис. 3).

Відповідно до теореми Стайнспрінга [3], операція Єви на лінії Боб $\rightarrow$ Аліса може бути реалізована унітарним оператором у гільбертовому просторі проб H_E, розмірність якого задовольняє умові $\dim H_E \le (\dim H_B)^2$, де $\dim H_B$ – розмірність гільбертового простору передаваних Бобом двох кубітів ($\dim H_B = 4$). Таким чином, Єва може використати для атаки чотирикубітні проби ($\dim H_E = 16$), і атака з використанням таких проб буде найбільш загальною.

Стан пари кубітів, що посилає Боб, є повністю змішаним, його редукована матриця щільності $\rho_B = Tr_{3,4}(|\Omega_1\rangle\langle\Omega_1|) = \bar{I}/4$, де індекси «3» та «4» у символі операції «частковий слід» позначають номери кубітів, за якими береться слід; $\bar{I}$ – одинична матриця розміром 4×4. Тому для аналізу атаки можна вважати, що Боб посилає пару кубітів в одному зі станів $|00\rangle$, $|01\rangle$, $|10\rangle$ або $|11\rangle$ з однаковою ймовірністю 1/4.

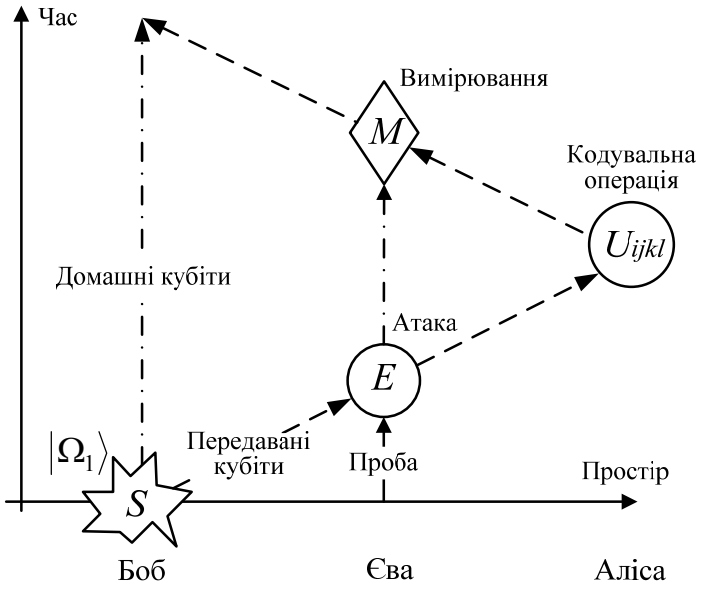

Рисунок 3 – Схема атаки пасивного перехоплення

Таким чином, стани складеної системи "передавані кубіти – проба Єви" після атаки можуть бути записані у виді:

$$\left|\psi^{(1)}\right\rangle = \widehat{E}\left|00,\varphi\right\rangle = \alpha_1\left|00,\varphi_{0000}\right\rangle + \beta_1\left|01,\varphi_{0001}\right\rangle + \gamma_1\left|10,\varphi_{0010}\right\rangle + \delta_1\left|11,\varphi_{0011}\right\rangle;$$

$$\left|\psi^{(2)}\right\rangle = \widehat{E}\left|01,\varphi\right\rangle = \alpha_2\left|00,\varphi_{0100}\right\rangle + \beta_2\left|01,\varphi_{0101}\right\rangle + \gamma_2\left|10,\varphi_{0110}\right\rangle + \delta_2\left|11,\varphi_{0111}\right\rangle;$$

$$\left|\psi^{(3)}\right\rangle = \widehat{E}\left|10,\varphi\right\rangle = \alpha_3\left|00,\varphi_{1000}\right\rangle + \beta_3\left|01,\varphi_{1001}\right\rangle + \gamma_3\left|10,\varphi_{1010}\right\rangle + \delta_3\left|11,\varphi_{1011}\right\rangle;$$

$$\left|\psi^{(4)}\right\rangle = \widehat{E}\left|11,\varphi\right\rangle = \alpha_4\left|00,\varphi_{1100}\right\rangle + \beta_4\left|01,\varphi_{1101}\right\rangle + \gamma_4\left|10,\varphi_{1110}\right\rangle + \delta_4\left|11,\varphi_{1111}\right\rangle, \quad (3)$$

де $\left\{\left|\varphi_{ijkl}\right\rangle\right\}$ – множина станів проби Єви.

З умови унітарності операції $\widehat{E}$ випливають такі співвідношення між параметрами проби:

$$\alpha_i^*\alpha_j + \beta_i^*\beta_j + \gamma_i^*\gamma_j + \delta_i^*\delta_j = \varepsilon_{ij}, \quad (4)$$

де ε_{ij} – символ Кронекера, $i = 1...4$, $j = 1...4$.

Також через те, що стан передаваних кубітів повністю змішаний, повинні виконуватися наступні співвідношення:

$$|\alpha_1|^2 = |\beta_2|^2 = |\gamma_3|^2 = |\delta_4|^2; \quad |\alpha_2|^2 = |\beta_3|^2 = |\gamma_4|^2 = |\delta_1|^2;$$
$$|\alpha_3|^2 = |\beta_4|^2 = |\gamma_1|^2 = |\delta_2|^2; \quad |\alpha_4|^2 = |\beta_1|^2 = |\gamma_2|^2 = |\delta_3|^2. \quad (5)$$

Розглянемо спочатку випадок, коли Боб «посилає» $\left|00\right\rangle$, тобто стан квантової системи "передавані кубіти – проба Єви" після атаки стає $\left|\psi^{(1)}\right\rangle$ (див. (3)). Інші випадки в (3) розглядаються аналогічно.

Після виконання Алісою кодувальних операцій U_{0000}, U_{0001}, U_{0010}, U_{0011}, … (2) з частотами p_1, p_2, p_3, p_4, … відповідно, оператор щільності системи "передавані кубіти – проба Єви" має вид:

$$\rho^{(1)} = \sum_{i=1}^{16} p_i \left|\psi_i^{(1)}\right\rangle\left\langle\psi_i^{(1)}\right|, \quad (6)$$

де

$$\left|\psi_1^{(1)}\right\rangle = U_{0000}\left|\psi^{(1)}\right\rangle = \alpha_1\left|00,\varphi_{0000}\right\rangle + \beta_1\left|01,\varphi_{0001}\right\rangle + \gamma_1\left|10,\varphi_{0010}\right\rangle + \delta_1\left|11,\varphi_{0011}\right\rangle,$$

$$\left|\psi_2^{(1)}\right\rangle = U_{0001}\left|\psi^{(1)}\right\rangle = \alpha_1\left|00,\varphi_{0000}\right\rangle - \beta_1\left|01,\varphi_{0001}\right\rangle + \gamma_1\left|10,\varphi_{0010}\right\rangle - \delta_1\left|11,\varphi_{0011}\right\rangle,$$
$$\left|\psi_3^{(1)}\right\rangle = U_{0010}\left|\psi^{(1)}\right\rangle = \alpha_1\left|00,\varphi_{0000}\right\rangle + \beta_1\left|01,\varphi_{0001}\right\rangle - \gamma_1\left|10,\varphi_{0010}\right\rangle - \delta_1\left|11,\varphi_{0011}\right\rangle,$$
$$\left|\psi_4^{(1)}\right\rangle = U_{0011}\left|\psi^{(1)}\right\rangle = \alpha_1\left|00,\varphi_{0000}\right\rangle - \beta_1\left|01,\varphi_{0001}\right\rangle - \gamma_1\left|10,\varphi_{0010}\right\rangle + \delta_1\left|11,\varphi_{0011}\right\rangle,$$
$$\left|\psi_5^{(1)}\right\rangle = U_{0100}\left|\psi^{(1)}\right\rangle = \alpha_1\left|01,\varphi_{0000}\right\rangle + \beta_1\left|00,\varphi_{0001}\right\rangle + \gamma_1\left|11,\varphi_{0010}\right\rangle + \delta_1\left|10,\varphi_{0011}\right\rangle,$$
$$\left|\psi_6^{(1)}\right\rangle = U_{0101}\left|\psi^{(1)}\right\rangle = -\alpha_1\left|01,\varphi_{0000}\right\rangle + \beta_1\left|00,\varphi_{0001}\right\rangle - \gamma_1\left|11,\varphi_{0010}\right\rangle + \delta_1\left|10,\varphi_{0011}\right\rangle,$$
$$\left|\psi_7^{(1)}\right\rangle = U_{0110}\left|\psi^{(1)}\right\rangle = \alpha_1\left|01,\varphi_{0000}\right\rangle + \beta_1\left|00,\varphi_{0001}\right\rangle - \gamma_1\left|11,\varphi_{0010}\right\rangle - \delta_1\left|10,\varphi_{0011}\right\rangle,$$
$$\left|\psi_8^{(1)}\right\rangle = U_{0111}\left|\psi^{(1)}\right\rangle = -\alpha_1\left|01,\varphi_{0000}\right\rangle + \beta_1\left|00,\varphi_{0001}\right\rangle + \gamma_1\left|11,\varphi_{0010}\right\rangle - \delta_1\left|10,\varphi_{0011}\right\rangle,$$
$$\left|\psi_9^{(1)}\right\rangle = U_{1000}\left|\psi^{(1)}\right\rangle = \alpha_1\left|10,\varphi_{0000}\right\rangle + \beta_1\left|11,\varphi_{0001}\right\rangle + \gamma_1\left|00,\varphi_{0010}\right\rangle + \delta_1\left|01,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{10}^{(1)}\right\rangle = U_{1001}\left|\psi^{(1)}\right\rangle = \alpha_1\left|10,\varphi_{0000}\right\rangle - \beta_1\left|11,\varphi_{0001}\right\rangle + \gamma_1\left|00,\varphi_{0010}\right\rangle - \delta_1\left|01,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{11}^{(1)}\right\rangle = U_{1010}\left|\psi^{(1)}\right\rangle = -\alpha_1\left|10,\varphi_{0000}\right\rangle - \beta_1\left|11,\varphi_{0001}\right\rangle + \gamma_1\left|00,\varphi_{0010}\right\rangle + \delta_1\left|01,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{12}^{(1)}\right\rangle = U_{1011}\left|\psi^{(1)}\right\rangle = -\alpha_1\left|10,\varphi_{0000}\right\rangle + \beta_1\left|11,\varphi_{0001}\right\rangle + \gamma_1\left|00,\varphi_{0010}\right\rangle - \delta_1\left|01,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{13}^{(1)}\right\rangle = U_{1100}\left|\psi^{(1)}\right\rangle = \alpha_1\left|11,\varphi_{0000}\right\rangle + \beta_1\left|10,\varphi_{0001}\right\rangle + \gamma_1\left|01,\varphi_{0010}\right\rangle + \delta_1\left|00,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{14}^{(1)}\right\rangle = U_{1101}\left|\psi^{(1)}\right\rangle = -\alpha_1\left|11,\varphi_{0000}\right\rangle + \beta_1\left|10,\varphi_{0001}\right\rangle - \gamma_1\left|01,\varphi_{0010}\right\rangle + \delta_1\left|00,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{15}^{(1)}\right\rangle = U_{1110}\left|\psi^{(1)}\right\rangle = \alpha_1\left|11,\varphi_{0000}\right\rangle - \beta_1\left|10,\varphi_{0001}\right\rangle + \gamma_1\left|01,\varphi_{0010}\right\rangle + \delta_1\left|00,\varphi_{0011}\right\rangle,$$
$$\left|\psi_{16}^{(1)}\right\rangle = U_{1111}\left|\psi^{(1)}\right\rangle = \alpha_1\left|11,\varphi_{0000}\right\rangle - \beta_1\left|10,\varphi_{0001}\right\rangle - \gamma_1\left|01,\varphi_{0010}\right\rangle + \delta_1\left|00,\varphi_{0011}\right\rangle. \quad (7)$$

Максимальна кількість класичної інформації I_0, що доступна Єві після вимірювання над складеною системою "передавані кубіти – проба", визначається ентропією Холево [3]:

$$I_0 = S\left(\rho^{(1)}\right) - \sum_{i=1}^{16} p_i S\left(\rho_i^{(1)}\right) = S\left(\rho^{(1)}\right), \quad (8)$$

де $\rho_i^{(1)} = \left|\psi_i^{(1)}\right\rangle\left\langle\psi_i^{(1)}\right|$; S – ентропія фон Неймана й усі $S\left(\rho_i^{(1)}\right)$ дорівнюють нулю, тому що стани (7) – чисті. Таким чином,

$$I_0 = S\left(\rho^{(1)}\right) \equiv -Tr\left\{\rho^{(1)}\log_2\rho^{(1)}\right\} = -\sum_{i=1}^{16}\lambda_i\log_2\lambda_i \quad \text{(біт)}, \quad (9)$$

де λ_i – власні значення оператора щільності $\rho^{(1)}$ (6).

Величина I_0 показує, скільки інформації може отримати Єва за одну атакуючу операцію (після фінального вимірювання над системою "передавані кубіти – проба").

Для знаходження власних значень λ_i оператора щільності $\rho^{(1)}$ (6), цей оператор був записаний у матричному виді в такому ортогональному базисі:

$$\left\{\left|00,\varphi_{0000}\right\rangle, \left|01,\varphi_{0000}\right\rangle, \left|10,\varphi_{0000}\right\rangle, \left|11,\varphi_{0000}\right\rangle, \left|00,\varphi_{0001}\right\rangle, \left|01,\varphi_{0001}\right\rangle, \left|10,\varphi_{0001}\right\rangle, \left|11,\varphi_{0001}\right\rangle,\right.$$
$$\left.\left|00,\varphi_{0010}\right\rangle, \left|01,\varphi_{0010}\right\rangle, \left|10,\varphi_{0010}\right\rangle, \left|11,\varphi_{0010}\right\rangle, \left|00,\varphi_{0011}\right\rangle, \left|01,\varphi_{0011}\right\rangle, \left|10,\varphi_{0011}\right\rangle, \left|11,\varphi_{0011}\right\rangle\right\}. \quad (10)$$

Отримана матриця має розмір 16×16 і тут не приводиться через її громіздкість.

Рівняння 16-го степеня на власні значення розкладається на чотири рівняння 4-го степеня такого виду:

$$\lambda^4 + t_i\lambda^3 + z_i\lambda^2 + y_i\lambda + x_i = 0, \quad (11)$$

де i = 1…4, а коефіцієнти при i = 1 мають вид:

$$t_1 = -\left(p_1 + p_2 + p_3 + p_4\right),$$
$$z_1 = 4\left(p_1p_2 + p_3p_4\right)\left(\left|\alpha_1\right|^2\left|\beta_1\right|^2 + \left|\alpha_1\right|^2\left|\delta_1\right|^2 + \left|\beta_1\right|^2\left|\gamma_1\right|^2 + \left|\gamma_1\right|^2\left|\delta_1\right|^2\right) +$$

$$+4(p_1p_3+p_2p_4)\left(|\alpha_1|^2|\gamma_1|^2+|\alpha_1|^2|\delta_1|^2+|\beta_1|^2|\gamma_1|^2+|\beta_1|^2|\delta_1|^2\right)+$$
$$+4(p_1p_4+p_2p_3)\left(|\alpha_1|^2|\beta_1|^2+|\alpha_1|^2|\gamma_1|^2+|\beta_1|^2|\delta_1|^2+|\gamma_1|^2|\delta_1|^2\right),$$
$$y_1=-16(p_1p_2p_3+p_1p_2p_4+p_1p_3p_4+p_2p_3p_4)\left(|\alpha_1|^2|\beta_1|^2|\gamma_1|^2+|\alpha_1|^2|\beta_1|^2|\delta_1|^2+|\alpha_1|^2|\gamma_1|^2|\delta_1|^2+|\beta_1|^2|\gamma_1|^2|\delta_1|^2\right)$$
$$x_1=256p_1p_2p_3p_4|\alpha_1|^2|\beta_1|^2|\gamma_1|^2|\delta_1|^2. \qquad (12)$$

Решта коефіцієнтів виходять з вищенаведених заміною $p_1\to p_5$, $p_2\to p_6$, $p_3\to p_7$, $p_4\to p_8$ для $i=2$ (тобто, наприклад, $t_2=-(p_5+p_6+p_7+p_8)$ і т.д.); $p_1\to p_9$, $p_2\to p_{10}$, $p_3\to p_{11}$, $p_4\to p_{12}$ для $i=3$ та $p_1\to p_{13}$, $p_2\to p_{14}$, $p_3\to p_{15}$, $p_4\to p_{16}$ для $i=4$.

Аналогічно розглядаються інші випадки в (3), тобто коли замість $|00\rangle$ Боб «посилає» $|01\rangle$, $|10\rangle$, або $|11\rangle$. Для випадку $|10\rangle$ коефіцієнти рівнянь (11) співпадають с коефіцієнтами для $|00\rangle$, з урахуванням співвідношень (5), а для $|01\rangle$ та $|11\rangle$, також з урахуванням (5), мають вид:

$$t_1=-(p_1+p_2+p_3+p_4),$$
$$z_1=4(p_1p_2+p_3p_4)\left(|\alpha_1|^2|\beta_1|^2+|\alpha_1|^2|\delta_1|^2+|\beta_1|^2|\gamma_1|^2+|\gamma_1|^2|\delta_1|^2\right)+$$
$$+4(p_1p_3+p_2p_4)\left(|\alpha_1|^2|\beta_1|^2+|\alpha_1|^2|\gamma_1|^2+|\beta_1|^2|\delta_1|^2+|\gamma_1|^2|\delta_1|^2\right)+$$
$$+4(p_1p_4+p_2p_3)\left(|\alpha_1|^2|\gamma_1|^2+|\alpha_1|^2|\delta_1|^2+|\beta_1|^2|\gamma_1|^2+|\beta_1|^2|\delta_1|^2\right),$$
$$y_1=-16(p_1p_2p_3+p_1p_2p_4+p_1p_3p_4+p_2p_3p_4)\left(|\alpha_1|^2|\beta_1|^2|\gamma_1|^2+|\alpha_1|^2|\beta_1|^2|\delta_1|^2+|\alpha_1|^2|\gamma_1|^2|\delta_1|^2+|\beta_1|^2|\gamma_1|^2|\delta_1|^2\right)$$
$$x_1=256p_1p_2p_3p_4|\alpha_1|^2|\beta_1|^2|\gamma_1|^2|\delta_1|^2, \qquad (13)$$

і аналогічно для t_2, z_2 і т.д.

Як випливає з першого виразу в (3), у випадку, коли Боб «посилає» $|00\rangle$ і в режимі контролю підслуховування використовується вимірювальний базис B_z, тоді ймовірність виявити атаку

$$d_z=|\beta_1|^2+|\gamma_1|^2+|\delta_1|^2=1-|\alpha_1|^2. \qquad (14)$$

Аналогічно, якщо Боб «посилає» $|01\rangle$, $|10\rangle$ або $|11\rangle$, то

$$d_z=|\alpha_2|^2+|\gamma_2|^2+|\delta_2|^2=1-|\beta_2|^2=1-|\alpha_1^2|,\quad d_z=|\alpha_3|^2+|\beta_3|^2+|\delta_3|^2=1-|\gamma_3|^2=1-|\alpha_1^2|\ \text{ та}$$
$$d_z=|\alpha_4|^2+|\beta_4|^2+|\gamma_4|^2=1-|\delta_4|^2=1-|\alpha_1^2| \qquad (15)$$

відповідно, з урахуванням співвідношень (5). Таким чином, загальний вираз для ймовірності виявлення атаки при використанні в режимі контролю підслуховування базису B_z має вид (14).

Розглянемо далі *симетричну* атаку, тобто атаку за умов $|\beta_1|^2=|\gamma_1|^2=|\delta_1|^2=d_z/3$. В цьому випадку, використовуючи співвідношення (14), з формул для коефіцієнтів (12), (13) можна виключити параметри проб α_1, β_1, γ_1 і δ_1, увівши в ці формули ймовірність виявлення атаки d_z. Це дозволяє в остаточному підсумку виразити кількість інформації Єви I_0 (9) через d_z.

У випадку симетричної атаки, коефіцієнти рівнянь на власні значення (11) однакові поза залежністю від того, в якому зі станів ($|00\rangle$, $|01\rangle$, $|10\rangle$ або $|11\rangle$) Боб «посилає» кубіти, та при $i=1$ дорівнюють:

$$t_1=-(p_1+p_2+p_3+p_4),$$
$$z_1=4(p_1p_2+p_1p_3+p_1p_4+p_2p_3+p_2p_4+p_3p_4)\left[\frac{2}{3}(1-d_z)d_z+\frac{2}{9}d_z^2\right],$$

$$y_1 = -16\left(p_1p_2p_3 + p_1p_2p_4 + p_1p_3p_4 + p_2p_3p_4\right)\left[\frac{d_z^2}{3}\left(1-d_z\right)+\frac{d_z^3}{27}\right],$$

$$x_1 = 256p_1p_2p_3p_4\,\frac{d_z^3}{27}\left(1-d_z\right) \qquad (16)$$

і аналогічно для t_2, z_2, y_2, … (див. текст після формули (12)).

На рис. 4 наведені залежності кількості інформації I_0 Єви від ймовірності виявлення атаки d_z для симетричної атаки та різних значень частот $p_1 \dots p_{16}$ кодувальних операцій Аліси. Значення частот $p_1 \dots p_{16}$, а також ентропія $H = -\sum_{i=1}^{16} p_i \log_2 p_i$ двійкового коду для кривих на рис. 4 наведені в табл. 2. Для отримання цих кривих відповідні значення коефіцієнтів (16) підставлялись в рівняння на власні значення матриці щільності (11), потім ці рівняння розв'язувались чисельно і отримані шістнадцять власних значень підставлялись в (9).

Таблиця 2 – Частоти чотириграм $p_1 \dots p_{16}$ та ентропія H (біт/чотириграми) двійкового коду

Частоти	№ кривої на рис. 4						
	1	2	3	4	5	6	7
p_1	1/16	9/80	1/8	1/4	1/5	1/4	4/5
p_2	1/16	1/80	0	1/4	1/100	1/4	0
p_3	1/16	9/80	1/8	1/4	1/100	1/4	0
p_4	1/16	1/80	0	1/4	3/100	1/4	1/5
p_5	1/16	9/80	1/8	0	7/20	0	0
p_6	1/16	1/80	0	0	1/5	0	0
p_7	1/16	9/80	1/8	0	1/10	0	0
p_8	1/16	1/80	0	0	1/10	0	0
p_9	1/16	9/80	1/8	1/4	0	0	0
p_{10}	1/16	1/80	0	1/4	0	0	0
p_{11}	1/16	9/80	1/8	1/4	0	0	0
p_{12}	1/16	1/80	0	1/4	0	0	0
p_{13}	1/16	9/80	1/8	0	0	0	0
p_{14}	1/16	1/80	0	0	0	0	0
p_{15}	1/16	9/80	1/8	0	0	0	0
p_{16}	1/16	1/80	0	0	0	0	0
H	4,0	3,469	3,0	3,0	2,408	2,0	0,722

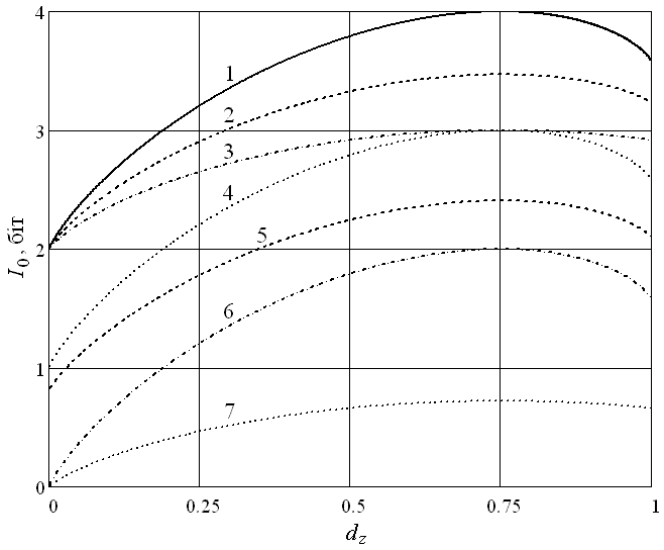

Рисунок 4 – Залежність інформації Єви I_0 (9)
від ймовірності d_z виявлення атаки при вимірюваннях в базисі B_z

Як видно з рис. 4, повну інформацію, яка дорівнює ентропії джерела, Єва отримує при $d_z = 0{,}75$. При $d_z > 0{,}75$ кількість інформації Єви починає зменшуватись. Тому, це значення ймовірності виявлення атаки можна вважати максимальним, оскільки Єва не буде вибирати параметри своїх допоміжних квантових систем так, щоб ймовірність виявлення атаки збільшувалась при зменшенні доступної їй інформації. Порівнюючи це значення d_z з відповідним значенням максимальної ймовірності виявлення атаки для протоколу з ГХЦ-четвірками кубітів ($d_z = 0{,}875$ [2]), можна дійти висновку, що при однаковій інформаційній місткості цих двох варіантів пінг-понг протоколу, протокол з ГХЦ-четвірками забезпечує дещо більшу максимальну ймовірність виявлення атаки. Але якщо Єва прагне зменшити ймовірність свого виявлення d_z за рахунок зменшення отримуваної нею інформації, то кількість інформації Єви буде менше для протоколу з кластерними станами, ніж для протоколу з ГХЦ-станами, в широкому діапазоні d_z, тобто в даному випадку протокол з кластерними станами забезпечує більш високий рівень стійкості. Цей факт проілюстрований на рис. 5, де показані залежності I_0 від d_z при однакових значеннях частот кодувальних операцій Аліси $p_1 = \ldots = p_{16} = 1/16$.

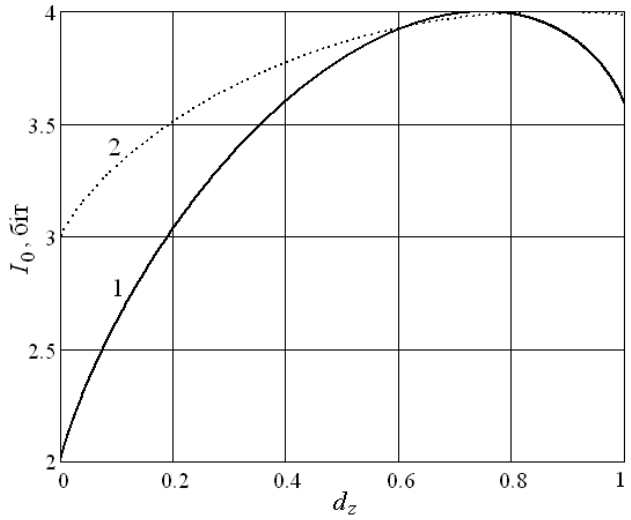

Рисунок 5 – Залежність інформації Єви I_0 від d_z для протоколу з чотирикубітними кластерними станами (1) та протоколу з чотирикубітними ГХЦ-станами (2)

Як видно з рис. 4, при $d_z = 0$ кількість інформації Єви не дорівнює нулю, але вона нижче свого максимального значення при $d_z = 0{,}75$. Таким чином, для пінг-понг протоколу з кластерними Ω -станами існує «невидимий» режим підслуховування, при якому Єва одержує часткову інформацію, але її операції не можуть бути виявлені легітимними користувачами, коли вони використовують у режимі контролю підслуховування тільки один вимірювальний базис B_z. Відзначимо, що аналогічна ситуація має місце й для пінг-понг протоколів з багатокубітними ГХЦ-станами [2] та протоколу з белівськими станами пар кутритів [9]. Як показано в [2, 4, 5, 9], для цих протоколів можливість такої «невидимої» атаки усувається при використанні легітимними користувачами в режимі контролю підслуховування другого вимірювального базису B_x. Аналогічно це може бути показано і для протоколу з чотирикубітними Ω-станами. Для цього необхідно вивести вираз для d_x – ймовірності виявлення атаки при використанні в режимі контролю підслуховування базису B_x.

Через те, що стан пари кубітів, які посилає Боб, повністю змішаний, тепер можна вважати, що Боб посилає пару кубітів в одному зі станів $|++\rangle$, $|+-\rangle$, $|-+\rangle$ або $|--\rangle$. Тоді формули (3) заміняються на наступні:

$$\begin{aligned}
|\psi^{(1)}\rangle &= \widehat{E}|++,\varphi\rangle = a_1|++,\varphi_{++++}\rangle + b_1|+-,\varphi_{+++-}\rangle + c_1|-+,\varphi_{++-+}\rangle + d_1|--,\varphi_{++--}\rangle;\\
|\psi^{(2)}\rangle &= \widehat{E}|+-,\varphi\rangle = a_2|++,\varphi_{+-++}\rangle + b_2|+-,\varphi_{+-+-}\rangle + c_2|-+,\varphi_{+--+}\rangle + d_2|--,\varphi_{+---}\rangle;\\
|\psi^{(3)}\rangle &= \widehat{E}|-+,\varphi\rangle = a_3|++,\varphi_{-+++}\rangle + b_3|+-,\varphi_{-++-}\rangle + c_3|-+,\varphi_{-+-+}\rangle + d_3|--,\varphi_{-+--}\rangle;\\
|\psi^{(4)}\rangle &= \widehat{E}|--,\varphi\rangle = a_4|++,\varphi_{--++}\rangle + b_4|+-,\varphi_{--+-}\rangle + c_4|-+,\varphi_{---+}\rangle + d_4|--,\varphi_{----}\rangle. \qquad (17)
\end{aligned}$$

Далі, всі формули (4)…(13) залишаються справедливими при заміні $\alpha_1 \to a_1$, $\beta_1 \to b_1$, $\gamma_1 \to c_1$, $\delta_1 \to d_1$, $|00\rangle \to |++\rangle$, $|01\rangle \to |+-\rangle$, $|10\rangle \to |-+\rangle$, $|11\rangle \to |--\rangle$, $\varphi_{0000} \to \varphi_{++++}$, $\varphi_{0001} \to \varphi_{+++-}$, $\varphi_{0010} \to \varphi_{++-+}$ і т.д. Таким чином, вираз (14) переходить у вираз

$$d_x = |b_1|^2 + |c_1|^2 + |d_1|^2 = 1 - |a_1|^2. \qquad (18)$$

Використовуючи (3) та (17), можна отримати вирази, що зв'язують параметри α_1, β_1, γ_1 та δ_1 з параметрами a_1, b_1, c_1 та d_1:

$$\begin{aligned}
|\alpha_1|^2 &= \frac{1}{4}|a_1 + b_1 + c_1 + d_1|^2, \qquad & |\beta_1|^2 &= \frac{1}{4}|a_1 - b_1 + c_1 - d_1|^2,\\
|\gamma_1|^2 &= \frac{1}{4}|a_1 + b_1 - c_1 - d_1|^2, \qquad & |\delta_1|^2 &= \frac{1}{4}|(a_1 - b_1 - c_1 + d_1)|^2. \qquad (19)
\end{aligned}$$

Використовуючи тепер (14), (18) та (19) можна показати, що при будь-якому значенні величини d_z величина d_x дорівнює своєму максимальному значенню 0,75, і навпаки. Тим самим «невидимий» режим атаки пасивного перехоплення усувається при використанні в режими контролю підслуховування двох взаємно незміщених вимірювальних базисів, як і для інших варіантів пінг-понг протоколу.

На закінчення відзначимо наступне. У роботі проаналізована атака пасивного перехоплення на пінг-понг протокол з чотирикубітними кластерними станами. Такий аналіз є одним з основних елементів синтезу квантової системи безпечного зв'язку, що ґрунтується на відповідному квантовому протоколі. Показано, що при використанні легітимними користувачами в режимі контролю підслуховування одного вимірювального базису існує «невидимий» режим перехвату інформації, при якому зловмисник одержує часткову інформацію, але його операції не можуть бути виявлені легітимними користувачами. Цей невидимий режим усувається при використанні двох взаємно незміщених вимірювальних базисів і, аналогічно пінг-понг протоколам з багатокубітними ГХЦ-станами, протокол з кластерними станами має асимптотичну стійкість до атаки пасивного перехоплення.

Максимальна ймовірність виявлення атаки за один раунд контролю підслуховування для протоколу з чотирикубітними кластерними станами дорівнює 0,75, що менше відповідної ймовірності для протоколу з чотирикубітними ГХЦ-станами, де вона дорівнює 0,875. Але у випадку, якщо зловмисник прагне зменшити ймовірність виявлення атаки за рахунок зменшення отримуваної інформації, протокол з кластерними станами забезпечує більш високий рівень стійкості до атаки пасивного перехоплення. Крім того, протокол з кластерними станами має перевагу над протоколом з ГХЦ-станами за рахунок більш ефективного використання квантового надщільного кодування: шістнадцять чотирикубітних кластерних станів можуть бути перетворені один в одного дією локальних унітарних операторів на два кубіти, тоді як для перетворення чотирикубітних ГХЦ-станів необхідно діяти на три кубіти. Це означає, що, відповідно до схеми пінг-понг протоколу, в протоколі з кластерними станами потрібно пересилати квантовим каналом меншу кількість кубітів, що підвищує стійкість протоколу до природних завад у каналі. Таким чином, можна зробити висновок, що протокол з чотирикубітними кластерними станами, маючи таку ж інформаційну місткість, як і протокол з чотирикубітними ГХЦ-станами (4 біти на один раунд), має більше переваг перед протоколом з ГХЦ-станами, ніж недоліків, і тому з цих двох варіантів пінг-понг протоколу є кращим для побудови квантової системи безпечного зв'язку.

Література

1. *Баумейстер Д.* Физика квантовой информации / Баумейстер Д., Экерт А., Цайлингер А. – М.: Постмаркет, 2002. – 376 с.
2. *Василиу Е.В.* Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009. – № 1. – С. 83–91.
3. *Нильсен М.* Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – М.: Мир, 2006. – 824 с.
4. *Bostrom K.* Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.
5. *Cai Q.-Y.* Improving the capacity of the Bostrom – Felbinger protocol / Q.-Y. Cai, B.-W. Li // Physical Review A. – 2004. – V. 69. – № 5. – 054301.
6. *Chamoli A.* Secure direct communication based on ping-pong protocol / A. Chamoli, C. Bhandari // Quantum Information Processing. – 2009. – V. 8. – № 4. – P. 347–356.
7. *Василиу Е.В.* Пинг-понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера / Е.В. Василиу, Л.Н. Василиу // Труды Одесского политехнического университета. – 2008. – Вып. 1(29). – С. 171–176.
8. *Василіу Є.В.* Пінг-понг протокол з повністю переплутаними станами пар та триплетів тривимірних квантових систем / Є.В. Василіу // Цифрові технології. – 2009. – № 5. – С. 18–26.
9. *Vasiliu E.V.* General individual attack on the ping-pong protocol with completely entangled pairs of qutrits [Електронний ресурс] / E.V. Vasiliu. – Режим доступу: http://arxiv.org/abs/0910.2002.
10. *Василиу Е.В.* Пинг-понг протокол квантовой безопасной связи с четырехкубитными кластерными состояниями / Е.В. Василиу, Р.С. Мамедов // Сборник научных трудов по материалам международной научно-практической конференции "Современные направления теоретических и прикладных исследований '2010".– Т. 3: Технические науки.– Одесса: Черноморье, 2010.– С. 20–25.