УДК 004.056.53 +530.145

ПОСЛІДОВНА АТАКА ПАСИВНОГО ПЕРЕХОПЛЕННЯ ДВОХ ЗЛОВМИСНИКІВ НА ПІНГ-ПОНГ ПРОТОКОЛ З ГХЦ-ТРИПЛЕТАМИ КУБІТІВ

Євген Василіу

У статті проаналізовано послідовну атаку пасивного перехоплення двох зловмисників на пінг-понг протокол з трикубітними переплутаними станами Грінбергера – Хорна – Цайлінгера. Одержано вираз для ймовірності виявлення атаки легітимними користувачами при атаці двох зловмисників у залежності від імовірностей виявлення їх атак окремо. Показано, що збільшення кількості атакуючих в квантовому каналі призводить до збільшення ймовірності виявлення їх атаки легітимними користувачами. Одержано вирази для максимальної кількості інформації двох зловмисників при їх послідовній атаці пасивного перехоплення на пінг-понг протокол з ГХЦ-триплетами. Показано, що максимальна кількість інформації зловмисників визначається тим же виразом, що й у випадку атаки одного зловмисника, змінюється тільки вираз для ймовірність виявлення атаки. Показано, що пінг-понг протокол з ГХЦ-триплетами вразливий до атаки пасивного перехоплення двох зловмисників не більше, ніж до атаки одного. Показано, що результати роботи можуть бути поширені на пінг-понг протоколи з n-кубітними ГХЦ-станами при довільних n.

Ключевые слова: *квантова криптографія, пінг-понг протокол, трикубітні стани Грінбергера – Хорна – Цайлінгера, атака пасивного перехоплення двох зловмисників, імовірність виявлення атаки, кількість інформації зловмисників.*

Вступ. У сучасному світі передача конфіденційних даних в мережах зв'язку може призвести як до втрати переданої інформації, так і до її компрометації, тобто розголошення інформації, що стала відомою якійсь особі, яка не має права доступу до неї. В останні два десятиліття активно розвивається новий напрямок захисту інформації, яка передається мережами зв'язку, – так звана квантова криптографія. На відміну від методів асиметричної криптографії, безпека яких ґрунтується на недоведених математичних твердженнях, безпека квантової криптографії ґрунтується на законах квантової фізики [1]. В квантовій криптографії для передачі інформації використовують фізичні об'єкти, що підкоряються законам квантової механіки. З практичної точки зору такими об'єктами є окремі фотони, які пересилають волоконно-оптичними лініями зв'язку.

Одним із напрямків квантової криптографії є протоколи квантового прямого безпечного зв'язку (КПБЗ), які дозволяють передавати конфіденційні повідомлення безпосередньо через відкритий квантовий канал, тобто без використання шифрування. На сьогодні запропонована велика кількість різних за призначенням протоколів КПБЗ [1–15]. Окремою групою таких протоколів, які не потребують квантової пам'яті великого обсягу для своєї практичної реалізації, є пінг-понг протоколи, що використовують різні переплутані стани двох та більшої кількості квантових систем (кубітів, кутритів і т.д.) [6–15].

На цей час досліджена стійкість деяких пінг-понг протоколів до різних видів атак, зокрема до атаки пасивного перехоплення з використанням допоміжних квантових систем (проб) [6, 7, 9, 11, 12]. Також виконано аналіз стійкості найпростішого пінг-понг протоколу з парами переплутаних кубітів до послідовної атаки пасивного перехоплення двох та більшої кількості зловмисників, які не знають про атаку один одного [15]. Але питання про стійкість до такої атаки більш складних пінг-понг протоколів з багатокубітними переплутаними станами раніше не розглядалось.

Метою цієї роботи є аналіз послідовної атаки пасивного перехоплення двох зловмисників на пінг-понг протокол з переплутаними трикубітними станами Грінбергера – Хорна – Цайлінгера (ГХЦ).

Загальна схема пінг-понг протоколу з трикубітними ГХЦ-станами. Пінг-понг протокол є двостороннім протоколом квантового безпечного зв'язку – для передавання повідомлення від одного абонента (Аліси) до іншого абонента (Боба) кубіти пересилаються спочатку від Боба до Аліси, а потім назад від Аліси до Боба. В пінг-понг протоколі застосовуються два режими – режим передавання самого повідомлення і режим контролю підслуховування, необхідний для виявлення атаки пасивного перехоплення. Аліса і Боб чергують ці режими випадковим чином. Атака детектується з деякою імовірністю в режимі контролю підслуховування. Агентів, які виконують атаку пасивного перехоплення, будемо називати зловмисниками – Євою$_1$ та Євою$_2$ (від англійського "eavesdropper" – агент, що підслуховує).

Ідея кодування класичної інформації в пінг-понг протоколах полягає в тому, що кожній групі класичних бітів відповідає окремий квантовий стан. При цьому різним групам бітів повинні

відповідати ортогональні стани. Це дозволяє, виконуючи проективні вимірювання у відповідному базисі, точно розрізняти ці стани і, тім самим, точно визначати відправлену групу бітів. Так, існує вісім ортогональних трикубітних станів ГХЦ, що дозволяє кодувати одним станом три класичних біти [10, 11]. В табл. 1 наведена відповідна схема квантового кодування. В цей табл. I – тотожній оператор, σ_x, σ_y, та σ_z – оператори Паулі.

Таблиця 1

Схема квантового кодування для пінг-понг протоколу з ГХЦ-триплетами

k	ГХЦ-стан	Оператор U_{ij} для перетворення $\lvert\Psi_1\rangle \to \lvert\Psi_k\rangle$, який діє на перші два кубіти $\lvert\Psi_1\rangle$	Трибітовий рядок, що відповідає $\lvert\Psi_k\rangle$
1	$\lvert\Psi_1\rangle = \left(\lvert 000\rangle + \lvert 111\rangle\right)/\sqrt{2}$	$I \otimes I$	000
2	$\lvert\Psi_2\rangle = \left(\lvert 000\rangle - \lvert 111\rangle\right)/\sqrt{2}$	$I \otimes \sigma_z$	001
3	$\lvert\Psi_3\rangle = \left(\lvert 100\rangle + \lvert 011\rangle\right)/\sqrt{2}$	$\sigma_x \otimes I$	010
4	$\lvert\Psi_4\rangle = \left(\lvert 100\rangle - \lvert 011\rangle\right)/\sqrt{2}$	$i\sigma_y \otimes I$	011
5	$\lvert\Psi_5\rangle = \left(\lvert 010\rangle + \lvert 101\rangle\right)/\sqrt{2}$	$I \otimes \sigma_x$	100
6	$\lvert\Psi_6\rangle = \left(\lvert 010\rangle - \lvert 101\rangle\right)/\sqrt{2}$	$I \otimes i\sigma_y$	101
7	$\lvert\Psi_7\rangle = \left(\lvert 110\rangle + \lvert 001\rangle\right)/\sqrt{2}$	$\sigma_x \otimes \sigma_x$	110
8	$\lvert\Psi_8\rangle = \left(\lvert 110\rangle - \lvert 001\rangle\right)/\sqrt{2}$	$i\sigma_y \otimes \sigma_x$	111

В пінг-понг протоколі з трикубітними ГХЦ-станами можна використовувати квантове надщільне кодування, тобто передавати три класичних біти, передаючи квантовим каналом два кубіти [10]. Квантове надщільне кодування дозволяє зменшити рівень помилок при передаванні в реальному квантовому каналі за рахунок зменшення кількості кубітів, що передаються.

На рис. 1 показана схема одного раунду режиму передавання повідомлення для пінг-понг протоколу з ГХЦ-триплетами. Боб, виготовивши стан $\lvert\Psi_1\rangle$, зберігає третій кубіт у себе в квантовій пам'яті ("домашній" кубіт), а перші два пересилає Алісі квантовим каналом. Аліса виконує кодувальну операцію над цими двома кубітами згідно з табл. 1 та посилає їх назад Бобові, який виконує вимірювання над усіма трьома кубітами в ГХЦ-базисі й тим самим визначає трибітову строку, що послала Аліса.

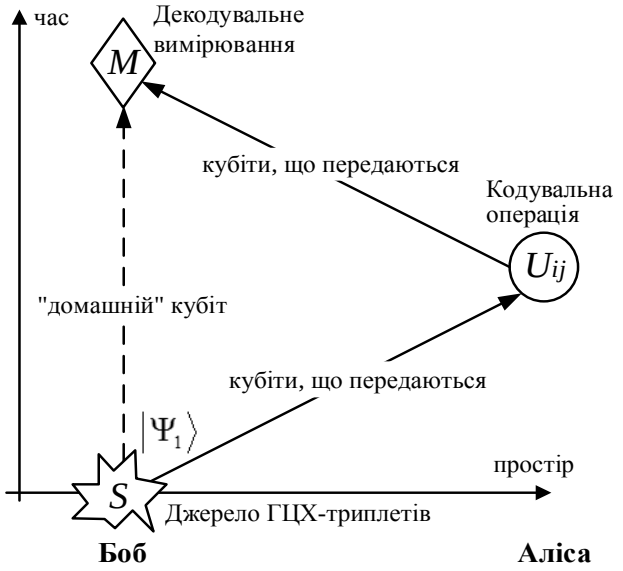

Рис. 1. Режим передавання повідомлення для пінг-понг протоколу з ГХЦ-триплетами кубітів

На рис. 2 показана схема одного раунду режиму контролю підслуховування. В цьому режимі легітимні сторони виконують проективні вимірювання над кубітами та обмінюються результатами звичайним (не квантовим) відкритим каналом зв'язку. Порівнюючи результати вимірювань, легітимні сторони можуть оцінити рівень помилок і, таким чином, виявити атаку пасивного перехоплення, якщо отриманий рівень помилок значно перевищує природній. Детальний опис режиму контролю підслуховування для пінг-понг протоколу з ГХЦ-триплетами наведено в [10, 11].

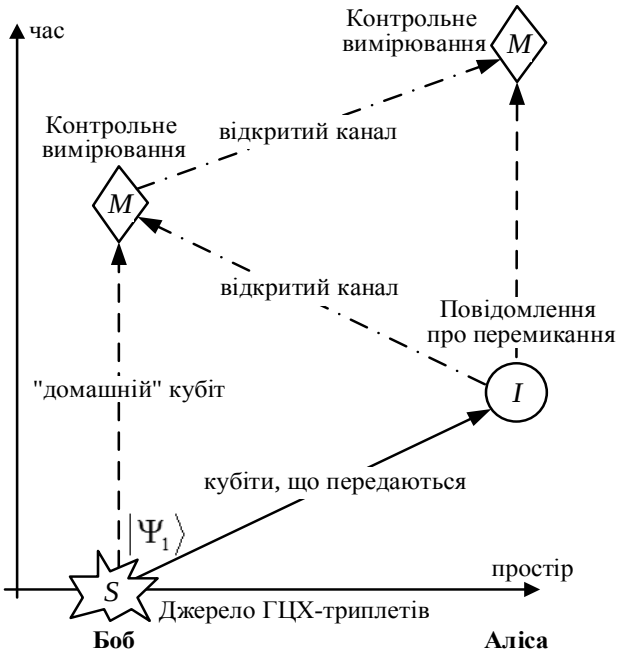

Рис. 2. Режим контролю підслуховування для пінг-понг протоколу з ГХЦ-триплетами кубітів

Режим контролю підслуховування в пінг-понг протоколі з трикубітними ГХЦ-станами при послідовній атаці пасивного перехоплення двох зловмисників. Для виконання такої атаки зловмисники повинні мати можливість, крім виконання операцій над окремими кубітами, також прослуховувати звичайний канал зв'язку між легітимними користувачами (рис. 3).

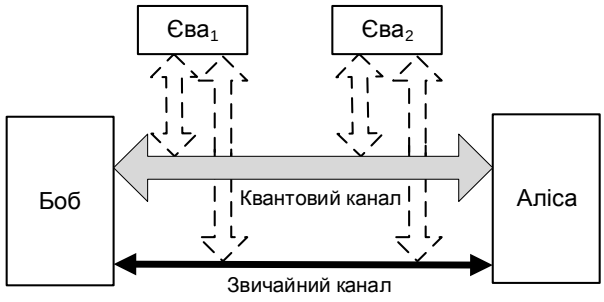

Рис. 3. Загальна схема атаки двох зловмисників на пінг-понг протокол з ГХЦ-триплетами

Оскільки атака зловмисників детектується в режимі контролю підслуховування, опишемо цей режим по крокам при наявності атаки двох зловмисників (рис. 4).

Крок 1. Боб приготовляє трикубітний стан $|\Psi_1\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$.

Крок 2. Боб залишає у себе в квантовій пам'яті один з трьох кубітів (наприклад, третій) та посилає Алісі перші два, використовуючи квантовий канал зв'язку.

Крок 3. $Єва_1$ переплутує два передаваних кубіти зі своєю допоміжною квантовою системою (пробою) і відправляє передавані кубіти далі квантовим каналом, а пробу зберігає у себе в квантовій пам'яті.

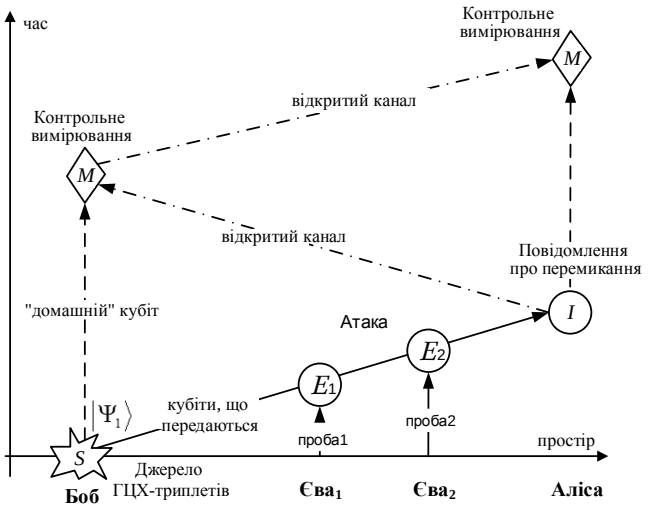

Рис. 4. Режим контролю підслуховування для пінг-понг протоколу з ГХЦ-триплетами при послідовній атаці двох зловмисників

Крок 4. $Єва_2$ перехоплює передавані кубіти (що вже знаходяться в переплутаному стані з пробою $Єви_1$) і переплутує їх зі своєю пробою, а потім відправляє ці два кубіти далі каналом зв'язку.

Крок 5. Аліса одержує два передаваних кубіти й повідомляє Бобові звичайним відкритим каналом зв'язку (з автентифікацією) про перехід до режиму контролю підслуховування. Відзначимо, що автентифікація всіх повідомлень, які передаються звичайним каналом зв'язку необхідна для того, що запобігти атаці "людина всередині", при якій зловмисники могли б замінити ці повідомлення й тим самим надати легітимним користувачам невірну статистику помилок в режимі контролю підслуховування. Це дозволило б зловмисникам замаскувати атаку пасивного перехоплення.

Крок 6. Боб випадковим чином вибирає один із двох однокубітних вимірювальних базисів – B_z або B_x, а потім виконує вимірювання стану свого кубіту в обраному базисі. Потім Боб повідомляє Алісі звичайним каналом обраний базис, а також повідомляє результат свого вимірювання (див. рис. 4).

Крок 7. Аліса виконує вимірювання станів двох своїх кубітів в тих же базисах, що вибрав Боб, та вони порівнюють результати своїх вимірювань. В ідеальному квантовому каналі зв'язку, якщо результати збігаються, то атаки немає й виконується наступний раунд протоколу, в протилежному випадку протокол переривається. Але в реальних каналах завжди є природні завади. Тому легітимні користувачі повинні виконати деяку кількість раундів контролю підслуховування (чергуючи їх з режимом передавання повідомлення), щоб одержати статистично значиму оцінку рівня помилок і порівняти її із заздалегідь відомим рівнем природних завад. Якщо одержаний рівень помилок значно перевищує природній, то робиться висновок про наявність атаки й протокол переривається.

Максимальна кількість інформації двох зловмисників при їх послідовній атаці пасивного перехоплення на пінг-понг протокол з ГЦХ-триплетами. Обчислимо тепер максимальну кількість інформації, яку можуть отримати два зловмисники в режимі передавання повідомлення в залежності від ймовірності виявлення їх атаки в режимі контролю підслуховування. Для цього узагальнімо аналіз атаки пасивного перехоплення одного зловмисника на пінг-понг протокол з ГХЦ-триплетами, виконаний в [11], на випадок послідовної атаки двох зловмисників.

$Єва_1$ не може відрізнити стан двох передаваних кубітів від повністю змішаного стану, так як

ці кубіти є частиною єдиного повністю переплутаного стану $|\Psi_1\rangle$. Відзначимо, що цей факт використовується в різних варіантах пінг-понг протоколу для запобігання атаки перехоплення та вимірювання станів передаваних кубітів – якщо зловмисник просто перехопить та вимірює стан передаваних кубітів, то він не отримає ніякої інформації, так як цей стан є повністю змішаним.

При атаці з використанням допоміжних квантових систем (див. рис. 4) вищезазначене відповідає для Єви$_1$ ситуації, якщо б суб'єкт *B* посилав передавані кубіти в одному з станів $|00\rangle$, $|01\rangle$, $|10\rangle$, або $|11\rangle$ з однаковою імовірністю $p=1/4$ [11]. Тоді стани складеної квантової системи "передавані кубіти – проба Єви$_1$" після атаки запишуться у вигляді:

$$
\begin{aligned}
|\psi^{(1)}\rangle &= \hat{E}_1|00,\varphi\rangle = \alpha_1|00,\varphi_{0000}\rangle + \beta_1|01,\varphi_{0001}\rangle + \gamma_1|10,\varphi_{0010}\rangle + \delta_1|11,\varphi_{0011}\rangle;\\
|\psi^{(2)}\rangle &= \hat{E}_1|01,\varphi\rangle = \alpha_2|00,\varphi_{0100}\rangle + \beta_2|01,\varphi_{0101}\rangle + \gamma_2|10,\varphi_{0110}\rangle + \delta_2|11,\varphi_{0111}\rangle;\\
|\psi^{(3)}\rangle &= \hat{E}_1|10,\varphi\rangle = \alpha_3|00,\varphi_{1000}\rangle + \beta_3|01,\varphi_{1001}\rangle + \gamma_3|10,\varphi_{1010}\rangle + \delta_3|11,\varphi_{1011}\rangle;\\
|\psi^{(4)}\rangle &= \hat{E}_1|11,\varphi\rangle = \alpha_4|00,\varphi_{1100}\rangle + \beta_4|01,\varphi_{1101}\rangle + \gamma_4|10,\varphi_{1110}\rangle + \delta_4|11,\varphi_{1111}\rangle,
\end{aligned}
\tag{1}
$$

де $\{|\varphi_{ijkl}\rangle\}$ – множина станів чотирикубітної проби Єви$_1$.

Матричне зображення атакуючої операції Єви$_1$ має вигляд

$$
\hat{E}_1 = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \gamma_1 & \gamma_2 & \gamma_3 & \gamma_4 \\ \delta_1 & \delta_2 & \delta_3 & \delta_4 \end{pmatrix}. \tag{2}
$$

З умови унітарності операції $\hat{E}_1$ випливають такі співвідношення між параметрами проби Єви$_1$:

$$
\alpha_i^*\alpha_j + \beta_i^*\beta_j + \gamma_i^*\gamma_j + \delta_i^*\delta_j = \varepsilon_{ij}, \tag{3}
$$

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

Також через те, що стан двох передаваних кубітів повністю змішаний, виконуються наступні співвідношення:

$$
\begin{aligned}
|\alpha_1|^2 &= |\beta_2|^2 = |\gamma_3|^2 = |\delta_4|^2;\\
|\alpha_2|^2 &= |\beta_3|^2 = |\gamma_4|^2 = |\delta_1|^2;\\
|\alpha_3|^2 &= |\beta_4|^2 = |\gamma_1|^2 = |\delta_2|^2;\\
|\alpha_4|^2 &= |\beta_1|^2 = |\gamma_2|^2 = |\delta_3|^2.
\end{aligned}
\tag{4}
$$

Розглянемо спочатку випадок, коли Боб посилає" $|00\rangle$, тобто стан квантової системи "передавані кубіти – проба Єви$_1$" після атаки $\hat{E}_1$ стає $|\psi^{(1)}\rangle$. Інші випадки у формулі (1) розглядаються аналогічно. Імовірність d_1 виявити атаку Єви$_1$ за один раунд контролю підслуховування за відсутності атаки Єви$_2$:

$$
d_1 = |\beta_1|^2 + |\gamma_1|^2 + |\delta_1|^2 = 1 - |\alpha_1|^2. \tag{5}
$$

Тоді, у випадку симетричної атаки: $|\beta_1|^2 = |\gamma_1|^2 = |\delta_1|^2$, коефіцієнти в $|\psi^{(1)}\rangle$ приймають вигляд: $\alpha_1 = \sqrt{1-d_1}$ та $\beta_1 = \sqrt{\frac{d_1}{3}}$, $\gamma_1 = \sqrt{\frac{d_1}{3}}$, $\delta_1 = \sqrt{\frac{d_1}{3}}$.

Будемо вважати, що Єва$_2$ не знає про атаку Єви$_1$ і виконує таку ж операцію переплутування двох передаваних кубітів зі своєю пробою, як і Єва$_1$, вважаючи, що ці два кубіти прийшли безпосередньо від Боба. Тоді після операції Єви$_2$

$$
\hat{E}_2 = \begin{pmatrix} \eta_1 & \eta_2 & \eta_3 & \eta_4 \\ \zeta_1 & \zeta_2 & \zeta_3 & \zeta_4 \\ \xi_1 & \xi_2 & \xi_3 & \xi_4 \\ \vartheta_1 & \vartheta_2 & \vartheta_3 & \vartheta_4 \end{pmatrix}, \tag{6}
$$

стан системи "передавані кубіти – проби зловмисників" буде мати вид:

$$
\begin{aligned}
|\psi'_{1(norm)}\rangle = \sqrt{1-d_1}\Big[&\sqrt{1-d_2}\,|00,\phi_{0000},\chi_{0000}\rangle + \\
&\sqrt{\frac{d_2}{3}}\,|01,\phi_{0000},\chi_{0001}\rangle + \\
&\sqrt{1-d_2}\,|10,\phi_{0000},\chi_{0010}\rangle + \sqrt{\frac{d_2}{3}}\,|11,\phi_{0000},\chi_{0011}\rangle\Big] + \\
\sqrt{\frac{d_1}{3}}\Big[&\sqrt{\frac{d_2}{3}}\,|00,\phi_{0001},\chi_{0100}\rangle + \sqrt{1-d_1}\,|01,\phi_{0001},\chi_{0101}\rangle + \\
&+\sqrt{\frac{d_2}{3}}\,|10,\phi_{0001},\chi_{0110}\rangle + \sqrt{\frac{d_2}{3}}\,|11,\phi_{0001},\chi_{0111}\rangle\Big] + \\
\sqrt{\frac{d_1}{3}}\Big[&\sqrt{\frac{d_2}{3}}\,|00,\phi_{0010},\chi_{1000}\rangle + \sqrt{\frac{d_2}{3}}\,|01,\phi_{0010},\chi_{1001}\rangle +
\end{aligned}
$$

$$+\sqrt{1-d_2}\,|10,\phi_{0010},\chi_{1010}\rangle+\sqrt{\frac{d_2}{3}}\,|11,\phi_{0010},\chi_{1011}\rangle\Bigg]+$$

$$\sqrt{\frac{d_1}{3}}\Bigg[\sqrt{\frac{d_2}{3}}\,|00,\phi_{0011},\chi_{1100}\rangle+\sqrt{\frac{d_2}{3}}\,|01,\phi_{0011},\chi_{1101}\rangle+$$

$$+\sqrt{1-d_2}\,|10,\phi_{0011},\chi_{1110}\rangle+\sqrt{\frac{d_2}{3}}\,|11,\phi_{0011},\chi_{1111}\rangle\Bigg], \quad (7)$$

де $\{|\chi_{ijkl}\rangle\}$ – множина станів проби Єви$_2$; $d_2=|\zeta_1|^2+|\xi_1|^2+|\vartheta_1|^2=1-|\eta_1|^2$ – імовірність виявити атаку Єви$_2$ за один раунд контролю підслуховування (при відсутності атаки Єви$_1$). У формулі (7) замість коефіцієнтів η_1, ζ_1, ξ_1 та ϑ_1 підставлені їх вирази через d_2, а саме: $\eta_1=\sqrt{1-d_2}$ та $\zeta_1=\xi_1=\vartheta_1=\sqrt{\frac{d_2}{3}}$.

Відзначимо, що хвильова функція (7) нормована. Вираз для величини d – імовірності виявити спільну послідовну атаку двох зловмисників за один раунд контролю підслуховування приймає вигляд:

$$d=1-\frac{\left(\sqrt{(1-d_1)(1-d_2)}+\sqrt{d_2\cdot d_1}\right)^2}{norm(d_1,d_2)}, \quad (8)$$

де нормуючий множник, необхідний для того, щоб імовірність d знаходилась в інтервалі від 0 до 1, має вид:

$$norm(d_1,d_2)=\left(\sqrt{(1-d_1)(1-d_2)}+\sqrt{d_2\cdot d_1}\right)^2+$$

$$3\left(\sqrt{\frac{(1-d_1)d_2}{3}}+\sqrt{\frac{(1-d_2)d_1}{3}}+\frac{2}{3}\sqrt{d_1d_2}\right)^2. \quad (9)$$

Обчислимо тепер максимальну кількість інформації, яку можуть отримати зловмисники Єва$_1$ та Єва$_2$, виконуючи свої атаки в режимі передавання повідомлення.

Максимальна кількість класичної інформації I_0, яка може бути отримана шляхом вимірювання квантового стану, визначається ентропією фон Неймана:

$$I_0=S(\rho_1'')\equiv -Tr[\rho_1''\log_2\rho_1'']=-\sum_i\lambda_i\log_2\lambda_i, \quad (10)$$

де ρ_1'' – матриця щільності стану системи "передавані фотони – проби зловмисників" після виконання Алісою кодувальних операцій; явний вираз для матриця щільності ρ_1'' тут не приводиться через його громіздкість; λ_i – власні значення матриця щільності ρ_1''.

Обчислення, виконані з використанням пакету символьних математичних обчислень Wolfram Mathematica 9, показують, що є вісім ненульових власних значень матриці щільності:

$$\lambda_{1,2}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2\cdot\frac{2}{3}d\left(1-\frac{2}{3}d\right)};$$

$$\lambda_{3,4}=\frac{1}{2}(p_3+p_4)\pm\frac{1}{2}\sqrt{(p_3+p_4)^2-16p_3p_4\cdot\frac{2}{3}d\left(1-\frac{2}{3}d\right)};$$

$$\lambda_{5,6}=\frac{1}{2}(p_5+p_6)\pm\frac{1}{2}\sqrt{(p_5+p_6)^2-16p_5p_6\cdot\frac{2}{3}d\left(1-\frac{2}{3}d\right)}; \quad (11)$$

$$\lambda_{7,8}=\frac{1}{2}(p_7+p_8)\pm\frac{1}{2}\sqrt{(p_7+p_8)^2-16p_7p_8\cdot\frac{2}{3}d\left(1-\frac{2}{3}d\right)},$$

де d визначається виразами (8), (9); p_1, …, p_8 – частоти кодувальних операцій Аліси, що представлені в табл. 1. У подальшому при розрахунку максимальної кількості інформації, яку можуть перехопити зловмисники, розглядається випадок $p_1=...=p_8=1/8$, якій відповідає передаванню даних, добре упакованих ентропійними методами стиску.

У випадку, коли Боб «посилає» $|01\rangle$, $|10\rangle$, або $|11\rangle$, розрахунки виконуються аналогічно вищевикладеним, і вирази (10), (11) залишаються незмінними. Отже остаточно, максимальна кількість інформації Єви$_2$ задається виразом (10), де λ_1, … λ_8 визначені в (11) і d визначено в (8), (9).

Порівнюючи одержані вирази (8) – (11) з відповідними виразами при атаці одного зловмисника на пінг-понг протокол з ГЦХ-триплетами кубітів [11], можна зробити висновок, що ці вирази мають однаковий вигляд, з тією лише різницею, що вирази для d – ймовірності виявлення атаки за один раунд контролю підслуховування – різні в цих випадках: у випадку атаки двох зловмисників d залежить від параметрів проб обох цих зловмисників. Відзначимо також, що аналогічний факт має місто й для пінг-понг протоколу з парами переплутаних кубітів [15].

Максимальна ймовірність виявлення атаки як одного зловмисника, так і двох для пінг-понг протоколу з ГЦХ-триплетами дорівнює 0,75.

Рис. 5 ілюструє залежності $d(d_1,d_2)$ (8) при заданих значеннях d_2. Видно, що другий зловмисник збільшує імовірність виявлення атаки легітимними користувачами, причому тим сильніше, чим більше інформації він хоче отримати. Також видно, що при d_2 = 0,75 величина d також дорів-

нює 0,75 і не залежить від d_1 (і навпаки, при d_1 = 0,75 величина d = 0,75 і не залежить від d_2). Це означає, що якщо другий зловмисник хоче отримати повну інформацію (що відповідає d_2 = 0,75), то перший зловмисник не може регулювати свою атаку (і навпаки).

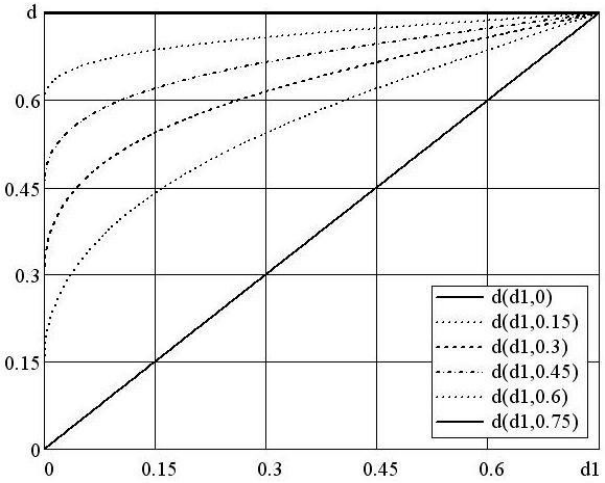

Рис. 5. Залежності ймовірності d виявлення атаки двох зловмисників від ймовірностей d_1 і d_2 виявлення їх атак окремо

На рис. 6 представлено залежність максимальної кількості інформації I_0 Єви$_2$ (10) при послідовних атаках двох зловмисників. Видно, що I_0 монотонно зростає із збільшенням як d_1, так і d_2. Видно також, що перший зловмисник як би "допомагає" другому, тобто другий може отримати більше інформації, ніж він очікує при заданому ним d_2. Однак величина d при цьому перевищує d_2 (див. рис. 5), тобто другий зловмисник, не знаючи про атаку першого, створить більшу імовірність виявлення його атаки, ніж він планував, задаючи d_2 шляхом регулювання параметрів своїх проб. Оскільки вирази (8), (9) для d є симетричним відносно d_1 і d_2, то й перший зловмисник, не знаючи про атаку другого, створить більшу імовірність виявлення атаки, ніж, якби він був один.

Як видно з рис. 6, при d_2 = 0,75, тобто коли Єва$_2$ прагне отримати повну інформацію, величина I_0 дорівнює 3 біти і не залежить від d_1, і навпаки. Це означає, що якщо Єва$_2$ організує свою атаку так, щоб отримати повну інформацію, то Єва$_1$ більше не зможе регулювати свою атаку, і навпаки.

Відзначимо, що залежність кількості інформації зловмисника, яка представлена на рис. 6, відповідає випадку, коли легітимні користувачі використовують один вимірювальний базис в режимі контролю підслуховування. В цьому випадку, як і при атаці одного зловмисника [11], існує "невидимий" режим підслуховування, коли зловмисник може отримати 2 біти інформації за 3-бітовий раунд протоколу, але його атака не буде виявлена легітимними користувачами. Однак, як і при атаці одного зловмисника [11], якщо легітимні користувачі будуть використовувати два взаємно незміщених базиси для вимірювань при контролі підслуховування, то можливість такої "невиявної" атаки зникає і у випадку двох зловмисників.

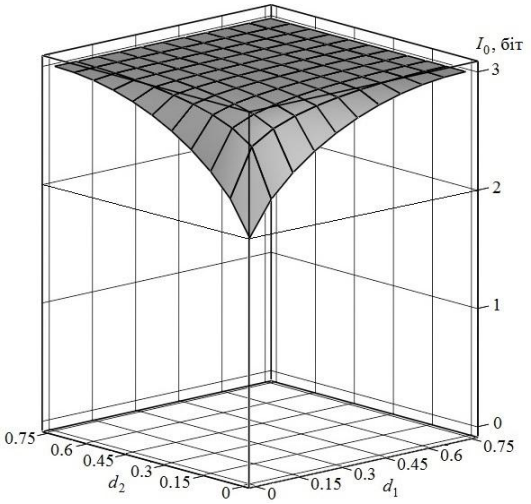

Рис. 6. Залежність максимальної кількості інформації I_0 Єви$_2$ при послідовній атаці двох зловмисників на протокол з ГХЦ-триплетами від ймовірностей d_1 і d_2 виявлення їх атак окремо

На рис. 7 для порівняння представлені залежності максимальної кількості інформації I_0 Єви$_2$ при послідовній атаці пасивного перехоплення двох зловмисників на пінг-понг протоколи з використанням двокубітних переплутаних станів Белла [15]. Нижня поверхня відповідає оригінальному протоколу без використання квантового надщільного кодування [6], який дозволяє передати один біт інформації за раунд, верхня поверхня – протоколу з квантовим надщільним кодуванням [9], що дозволяє передати два біти за раунд. Видно, що характер графіків на рис. 6 і 7 дуже схожий. Відмінності полягають тільки в кількості інформації, що передається за раунд протоколу, і відповідно в кількості перехопленої зловмисником інформації, а також в максимальній імовірності виявлення атаки, яка дорівнює 0,75 для протоколу з ГХЦ-триплетами і 0,5 для протоколів з парами Белла.

Відзначимо також, що внаслідок вимірювання, що виконується Євою$_2$ в режимі передавання повідомлення над складеною квантовою системою "передавані кубіти – проба" на шляху Аліса → Боб, стан цієї системи буде збурений, і відповідно максимальна кількість інформації Єви$_1$ буде не більше максимальної кількості інформації Єви$_2$, тобто Єва$_1$ в результаті атаки отримає не більше інформації, ніж її отримає Єва$_2$. При цьому, як випливає з (10), (11), ця кількість інформа-

ції визначається єдиною величиною – ймовірністю *d* виявлення атаки легітимними користувачами за один раунд контролю підслуховування, яка залежить від параметрів проб обох зловмисників згідно з (8), (9).

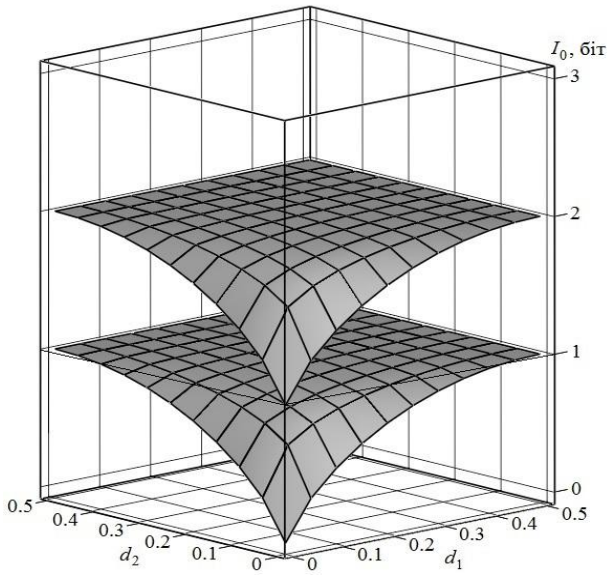

Рис. 7. Залежності максимальної кількості інформації I_0 Єви2 при атаці на пінг-понг протоколи зі станами Белла [15]

На підставі вищенаведених результатів порівняння стійкості пінг-понг протоколів з парами Белла та ГХЦ-триплетами кубітів до атаки пасивного перехоплення двох зловмисників можна зробити також наступне припущення. Показано [16], що для пінг-понг протоколів з *n*-кубітними ГХЦ-станами, які дозволяють передати *n* бітів інформації за раунд протоколу, кількість інформації *одного* зловмисника при його атаці пасивного перехоплення змінюється від *n* – 1 до *n* бітів, якщо легітимні користувачі використовують один вимірювальний базис в режимі контролю підслуховування. Тобто зловмисник одержує *n* – 1 бітів при "невиявної" атаці й від *n* – 1 до *n* бітів, коли збільшує ймовірність виявлення атаки *d*. При цьому максимальна ймовірність виявлення атака визначається виразом [16]:

$$d_{\max} = 1 - \frac{1}{2^{n-1}}. \qquad (12)$$

Як видно з рис. 6, 7, при атаці *двох* зловмисників на протоколи з переплутаними парами та ГХЦ-триплетами кубітів, їх інформація змінюється подібним ж чином. Тому можна зробити припущення, що при атаці пасивного перехоплення *двох* зловмисників на пінг-понг протоколи з *n*-кубітними ГХЦ-станами, інформація зловмисників також буде змінюватись від *n* – 1 до *n* бітів, а відповідні залежності будуть дуже подібні показаним на рис. 6 і 7. При цьому максимальна ймовірність виявлення атаки також буде визначатися виразом (12), наприклад, $d_{\max} = 0{,}875$ для пінг-понг протоколу з чотирикубітними ГЦХ-станами, який був детально розроблений в [10].

Висновки. У статті проаналізовано атаку пасивного перехоплення двох зловмисників на пінг-понг протокол з переплутаними трикубітними станами типу ГХЦ, коли зловмисники послідовно один за одним виконують операції над передаваними кубітами в квантовому каналі й не знають про атаки один одного. Виведено вираз для імовірності виявлення атаки легітимними користувачами при атаці двох зловмисників у залежності від ймовірностей виявлення їх атак окремо (тобто, якщо б перший проводив атаку за відсутності другого, або навпаки). Показано, що збільшення кількості атакуючих в квантовому каналі призводить до збільшення ймовірності виявлення їх атаки легітимними користувачами.

Одержано вирази для максимальної кількості інформації двох зловмисників при їх послідовній атаці на пінг-понг протокол з ГХЦ-триплетами. Показано, що максимальна кількість інформації другого зловмисника визначається тим же виразом, що й у випадку атаки одного зловмисника, змінюється тільки величина *d* – імовірність виявлення атаки легітимними користувачами. Максимальна кількість інформації першого зловмисника буде не більше максимальної кількості інформації другого.

Порівняльний аналіз атаки пасивного перехоплення двох зловмисників на пінг-понг протоколи з переплутаними парами кубітів та протокол з ГХЦ-триплетами кубітів дозволяє зробити обґрунтоване припущення, що характер зміни кількості інформації зловмисників при атаці на протоколи з *n*-кубітними ГХЦ-станами (при довільних *n*) буде аналогічний, а ця інформація буде знаходитись у межах від *n* – 1 до *n* бітів (при використанні легітимними користувачами одного вимірювального базису в режимі контролю підслуховування). Таким чином, результати цієї роботи можуть бути поширені на пінг-понг протоколи з *n*-кубітними ГХЦ-станами при довільних *n*.

Одержані результати свідчать про те, що пінг-понг протокол з ГХЦ-триплетами, також, як і протоколи з парами переплутаних кубітів [15], вразливий до атаки пасивного перехоплення двох зловмисників не більше, ніж до атаки одного. Два зловмисники не отримують жодних переваг, проводячи послідовно свої атаки в квантовому каналі зв'язку. Отже, у випадку, якщо зловмисники можуть домовитись між собою, найкращою

стратегією для них при атаці пасивного перехоплення на пінг-понг протоколи буде проводити одиночну атаку, а потім ділитися отриманою інформацією.

ЛИТЕРАТУРА

[1]. Deng F.G. Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block / F.G. Deng, G.L. Long, X.S. Liu / Physical Review A. – 2003. – V. 68, issue 4. – 042317.

[2]. Wang C. Multi – step quantum secure direct communication using multi – particle Greenberger – Horne – Zeilinger state / C. Wang, F.G. Deng, G.L. Long // Optics Communications. – 2005. – V. 253, issue 1. – P. 15-20.

[3]. Jin X.-R. Three-party quantum secure direct communication based on GHZ states / X.-R. Jin, X. Ji, Y.-Q. Zhang et al // Physics Letters A. – 2006. – V. 354, № 1-2. – P. 67-70.

[4]. Li X.-H. Multiparty Quantum Remote Secret Conference / X.-H. Li, C.-Y. Li, F.-G. Deng et al // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23-26.

[5]. Chamoli A. Secure direct communication based on ping-pong protocol / A. Chamoli, C.M. Bhandari // Quantum Information Processing. – 2009. – V. 8, num. 4. – P. 347-356.

[6]. Boström K. Deterministic secure direct communication using entanglement / K. Boström, T. Felbinger // Physical Review Letters. – 2002. – Vol. 89, issue 18. – 187902.

[7]. Cai Q.-Y. Improving the capacity of the Boström – Felbinger protocol / Q.-Y. Cai, B.-W. Li // Physical Review A. – 2004. – V. 69, issue 5. – 054301.

[8]. Ostermeyer, M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, issue 17. – P. 4540-4544.

[9]. Василиу Е.В. Анализ безопасности пинг-понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32-38.

[10]. 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.

[11]. Василиу Е.В. Анализ атаки на пинг – понг протокол с триплетами Гринбергера – Хорна – Цайлингера / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 15-24.

[12]. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // Quantum Information Processing. – 2011. – V. 10, num. 2. – P. 189-202.

[13]. Василиу Е.В. Три новых протокола квантовой безопасной связи с четырехкубитными кластерными состояниями / Е.В. Василиу, Р.С. Мамедов // Цифрові технології. – 2009. – № 6. – С. 94-103.

[14]. Мамедов Р.С. Пинг-понг протокол квантовой безопасной связи с четырехкубитными перепутанными W-состояниями / Р.С. Мамедов // Науково-технічний журнал «Захист інформації». – 2011, № 3(52). – С. 32-44.

[15]. Василіу Є.В. Аналіз послідовної атаки пасивного перехоплення декількох зловмисників на пінг-понг протокол з парами переплутаних кубітів / Є.В. Василіу, С.В. Ніколаєнко // Захист інформації. – 2013, Том 15, № 1(58). – С. 39-48.

[16]. 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.

REFERENCES

[1]. Deng F.G., Long G.L., Liu X.S. (2003) "Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block", *Physical Review A,* V. 68, issue 4, 042317.

[2]. Wang C., Deng F.G., Long G.L. (2005) "Multi-step quantum secure direct communication using multi – particle Greenberger – Horne – Zeilinger state" *Optics Communications,* V. 253, issue 1, P. 15-20.

[3]. Jin X.-R., Ji X., Y.-Q. Zhang et al (2006) "Three-party quantum secure direct communication based on GHZ states" *Physics Letters A,* V. 354, № 1-2, P. 67-70.

[4]. Li X.-H., Li C.-Y., Deng F.-G. et al (2007) "Multiparty Quantum Remote Secret Conference" *Chinese Physics Letters,* V. 24, № 1, P. 23-26.

[5]. Chamoli A., Bhandari C.M. (2009) "Secure direct communication based on ping-pong protocol" *Quantum Information Processing,* V. 8, num. 4, P. 347-356.

[6]. Boström K., Felbinger T. (2002) "Deterministic secure direct communication using entanglement" *Physical Review Letters,* Vol. 89, issue 18, 187902.

[7]. Cai Q.-Y., Li B.-W. (2004) "Improving the capacity of the Boström – Felbinger protocol" *Physical Review A,* V. 69, issue 5, 054301.

[8]. Ostermeyer M., Walenta N. (2008) "On the implementation of a deterministic secure coding protocol using polarization entangled photons" *Optics Communications,* V. 281, issue 17, P. 4540-4544.

[9]. Vasiliu E.V. (2007) "Security analysis of the ping-pong protocol with quantum dense coding" *Scientific works of ONAT n.a. Popov*, № 1, p. 32-38.
[10]. Vasiliu E.V., Vasiliu L.N. (2008) "Ping-pong protocol with tree- and four-qubit Greenberger-Horne-Zeilinger states" *Works of the Odessa polytechnic university*, No. 1(29), pp. 171-176.
[11]. Vasiliu E.V. (2008) "Analysis of attack on the ping-pong protocol with Greenberger – Horne – Zeilinger's triplets" *Scientific works of ONAT n.a. Popov*, № 1, pp. 15-24.
[12]. Vasiliu E.V. (2011) "Non-coherent attack on the ping-pong protocol with completely pairs of qutrits", *Quantum Information Processing* V. 10, num. 2, P. 189-202.
[13]. Vasiliu E.V., Mamedov R.S. (2009) "Three new protocols of quantum secure communication with four-qubit cluster states" *Digital*, № 6, p. 94-103.
[14]. Mamedov R.S. (2011) "Ping-pong protocol of QKD with entangled four-qubit W-states" *Ukrainian Information Security Research Journal*, № 3(52), pp. 32-44.
[15]. Vasiliu Ye.V., Nikolayenko S.V. (2013) "Analyses of the consistent eavesdropping attack of several eavesdroppers on the ping-pong protocol with entangled pairs of qubits" *Ukrainian Information Security Research Journal*, № 1(58), pp. 39-48.
[16]. Vasiliu Ye., Nikolayenko S. (2009) "Synthesis of structure of quantum secure direct communication systems" *Scientific works of ONAT n.a. Popov*, № 1, pp. 83-91.

ПОСЛЕДОВАТЕЛЬНАЯ АТАКА ПАССИВНОГО ПЕРЕХВАТА ДВУХ ЗЛОУМЫШЛЕННИКОВ НА ПИНГ-ПОНГ ПРОТОКОЛ С ГХЦ-ТРИПЛЕТАМИ КУБИТОВ

В статье проанализирована последовательная атака пассивного перехвата двух злоумышленников на пинг-понг протокол с трехкубитными перепутанными состояниями Гринбергера – Хорна – Цайлингера. Получено выражение для вероятности обнаружения атаки легитимными пользователями при атаке двух злоумышленников в зависимости от вероятностей обнаружения их атак отдельно. Показано, что увеличение количества атакующих в квантовом канале приводит к увеличению вероятности обнаружения их атаки легитимными пользователями. Получены выражения для максимального количества информации двух злоумышленников при их последовательной атаке пассивного перехвата на пинг-понг протокол с ГХЦ-триплетами. Показано, что максимальное количество информации злоумышленников определяется тем же выражением, что и в случае атаки одного злоумышленника, изменяется только выражение для вероятности обнаружения атаки. Показано, что пинг-понг протокол с ГХЦ-триплетами уязвим к атаке пассивного перехвата двух злоумышленников не больше, чем к атаке одного. Показано, что результаты работы могут быть распространены на пинг-понг протоколы с n-кубитными ГХЦ-состояниями при произвольных n.

Ключевые слова: квантовая криптография, пинг-понг протокол, трехкубитные состояния Гринбергера – Хорна – Цайлингера, атака пассивного перехвата двух злоумышленников, вероятность обнаружения атаки, количество информации злоумышленников.

CONSISTENT EAVESDROPPING ATTACK OF TWO EAVESDROPPERS ON THE PING-PONG PROTOCOL WITH GHZ-TRIPLETS OF QUBITS

In this paper has been analyzed the eavesdropping attack of two eavesdroppers on the ping-pong protocol with three-qubit entangled Greenberger – Horne – Zeilinger states. The expression for probability of attack detection by legitimate users at attack of two eavesdroppers depending on probabilities of detection them attacks separately are obtained. It is shown that an increase in the number of attackers in the quantum channel leads to an increase in the probability of detecting these attacks by legitimate users. The expressions for the maximum eavesdroppers' amount of information during a consistent attack of two eavesdroppers on the ping-pong protocol with GHZ-triplets are obtained. It is indicated that the maximum eavesdroppers' amount of information determined by the same expression as in the case of one eavesdropper's attack, only the expression for the probability of attack detection is changed. It is shown that the ping-pong protocol with GHZ-triplets is vulnerable to eavesdropping attack of two eavesdroppers not more than to one eavesdropper's attack. It is shown that results of paper could be extend to the ping-pong protocols with n-qubit GHZ-states at any n.

Keywords: quantum cryptography, a ping-pong protocol, three-qubit Greenberger – Horne – Zeilinger states, eavesdropping attack of two eavesdroppers, the probability of eavesdroppers' detection, eavesdroppers' amount of information.

Василіу Євген Вікторович, доктор технічних наук, доцент, директор Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки Одеської національної академії зв'язку ім. О.С. Попова.
E-mail: vasiliu@ua.fm
Василиу Евгений Викторович, доктор технических наук, доцент, директор Учебно-научного института Радио, телевидения и информационной безопасности Одесской национальной академии связи им. А.С. Попова.
Vasiliu Yevhen, Doctor of Science in Eng., Full Professor, Director of Educational and Research Institute of Radio, Television and Information Security of Odessa National Academy of Telecommunications n. a. O.S. Popov.