УДК 003.26:004.056.55:621.39

Корченко О.Г., Васіліу Є.В., Гнатюк С.О., Кінзерявий В.М.

ІМІТАЦІЙНА МОДЕЛЬ ПІНГ-ПОНГ ПРОТОКОЛУ З ПАРАМИ ПЕРЕПЛУТАНИХ КУТРИТІВ У КВАНТОВОМУ КАНАЛІ З ШУМОМ

Вступ. Квантова криптографія є одним з найважливіших і найбільш розвинених додатків квантової теорії інформації, що пропонує нові підходи до вирішення важливої проблеми передачі секретних повідомлень [1]. Один із напрямків квантової криптографії – це квантові протоколи прямого безпечного зв'язку, у яких взагалі не використовується шифрування, а таємність передачі гарантується законами квантової фізики [2–4]. Відкритий текст секретного повідомлення кодується за допомогою квантових станів груп квантових систем (дво- або багаторівневих), в якості котрих використовують фотони, а потім ці фотони передаються квантовим каналом зв'язку. При цьому закони квантової фізики гарантують виявлення підслуховування в каналі. Виявивши агента, що підслуховує (Єву), легітимні користувачі (Аліса й Боб) переривають сеанс зв'язку.

На даний час запропоновані різні види квантових протоколів безпечного зв'язку. Одним з таких протоколів є так званий пінг-понг протокол [2], який не потребує для своєї практичної реалізації великої квантової пам'яті і може виконуватися з використанням існуючого технічного обладнання [5]. У початковому варіанті пінг-понг протоколу використовуються два стани Бела переплутаної пари кубітів, що дозволяє передати один біт класичної інформації за один цикл протоколу [2]. Використання всіх чотирьох белівських станів пари кубітів, тобто квантового надщільного кодування, дозволяє передати два біти за цикл [3]. Подальше збільшення інформаційної місткості можливе при використанні замість переплутаних пар кубітів їх трійок, четвірок і т.д. Так, у роботі [4] був розроблений пінг-понг протокол з переплутаними станами Грінбергера-Хорна-Цайлінгера (ГХЦ) трійок та четвірок кубітів. Інформаційна місткість протоколу з такими станами дорівнює n бітів на цикл, де n – кількість кубітів у використовуваних ГХЦ-станах.

Інший шлях підвищення інформаційної місткості пінг-понг протоколу – це використання переплутаних станів багаторівневих квантових систем. Так, відповідний протокол з використанням станів Бела пари трирівневих систем (кутритів) та квантового надщільного кодування для кутритів був розроблений у роботах [6, 7]. Інформаційна місткість цього протоколу дорівнює $\log_2 9 \approx 3.17$ біт на цикл замість двох бітів на цикл для протоколу з белівськими станами кубітів.

Різні атаки, як на оригінальний пінг-понг протокол, так і на його вдосконалені варіанти, були розглянуті в ряді робіт [8–13]. Зокрема була проаналізована атака з використанням допоміжних квантових систем (загальна некогерентна атака) на різні варіанти пінг-понг протоколу, в тому числі на протокол з парами кутритів [8]. За такої атаки Єва може одержати деяку кількість інформації, перш ніж її атака буде виявлена [8, 11–13]. У роботі [13] запропоновано неквантовий спосіб підсилення безпеки пінг-понг протоколу, який полягає в оборотному гешуванні бітових блоків повідомлення множенням їх на випадкові оборотні матриці. Ці гешовані блоки передаються квантовим каналом і при цьому легітимні користувачі аналізують рівень помилок у режимі контролю підслуховування протоколу. Якщо цей рівень не перевищує допустимий, то звичайним (не квантовим) каналом передаються самі матриці, що дозволяє Бобові отримати текст повідомлення, множачи отримані блоки на відповідні обернені матриці.

Але для реалізації цього способу підсилення безпеки пінг-понг протоколу в каналі з природним квантовим шумом легітимним користувачам необхідно порівняти отриманий рівень помилок із заздалегідь відомим середнім рівнем шумів у даному квантовому каналі. При цьому внаслідок природи квантових помилок [14] атака Єви не буде просто додавати шум до природного, тобто рівні помилок, які виникають внаслідок операцій Єви та природних шумів, не будуть просто додаватись. Тому необхідно вирішити питання одночасного врахування зміни станів передаваних фотонів внаслідок операцій Єви та природного шуму. Це дозволить також побудувати відповідну імітаційну модель режиму

контролю підслуховування з метою отримання практичних рекомендацій щодо використання пінг-понг протоколу в каналі з шумом.

Метою цієї роботи є створення моделі режиму контролю підслуховування для пінг-понг протоколу з парами кутритів у каналі з шумом та імітаційне моделювання роботи цього протоколу в шумному каналі.

1. Режим контролю підслуховування для пінг-понг протоколу з парами повністю переплутаних кутритів

Детальний опис цього варіанту пінг-понг протоколу наведений в роботі [7]. Тут розглянемо тільки режим контролю підслуховування протоколу (рис. 1). У цьому режимі Аліса та Боб перевіряють збереженість початкового переплутаного стану $|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3}$, який приготовляє Боб, оскільки атака Єви призводить до зміни цього стану.

Як видно з рис. 1, стан кожного з кутритів вимірюється окремо – один Алісою, інший Бобом, а вимірювання необхідно виконувати в двох різних базисах, перемикаючись між ними випадковим чином. Наприклад, можна використовувати два взаємно незміщених базиси *z* та *x*:

$$|z_0\rangle = |0\rangle, \qquad |z_1\rangle = |1\rangle, \qquad |z_2\rangle = |2\rangle; \tag{1}$$

$$|x_0\rangle = \left(|0\rangle + |1\rangle + |2\rangle\right)/\sqrt{3},$$

$$|x_1\rangle = \left(|0\rangle + e^{2\pi i/3}|1\rangle + e^{-2\pi i/3}|2\rangle\right)/\sqrt{3}, \tag{2}$$

$$|x_2\rangle = \left(|0\rangle + e^{-2\pi i/3}|1\rangle + e^{2\pi i/3}|2\rangle\right)/\sqrt{3}.$$

Вимірювання Аліси в кожному з базисів дає один із трьох можливих результатів – "0", "1" або "2", кожний з імовірністю $1/3$. Одержавши від Аліси результат її вимірювання й обраний базис, Боб виконує вимірювання стану свого "домашнього" кутриту (див. рис. 1).

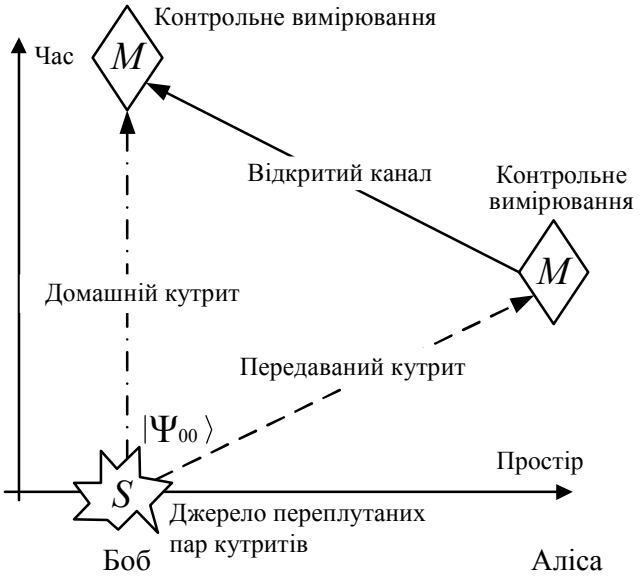


Рис. 1. Режим контролю підслуховування

Результат, який повинен отримати Боб (з одиничною ймовірністю), слідує із запису стану $|\Psi_{00}\rangle$ в *z*- та *x*-базисах [7]:

$$|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3} = \left(|x_0x_0\rangle + |x_1x_2\rangle + |x_2x_1\rangle\right)/\sqrt{3}. \tag{3}$$

Але завжди правильні результати вимірювань Боб буде одержувати тільки при відсутності як операцій Єви, так і природнього шуму в квантовому каналі. При їх наявності не існує способу розрізнити помилки, що виникають із цих двох причин [1]. З огляду на це, важливо побудувати модель, яка одночасно враховує як атаку Єви, так і природній

квантовий шум в каналі, що дозволить дати рекомендації щодо практичного використання пінг-понг протоколу в каналі з шумом.

2. Модель режиму контролю підслуховування в квантовому каналі з шумом

У класичній теорії передачі інформації, коли інформація передається бітами, єдиний можливий тип помилок, що може відбутися, – це переворот біта. У квантовому випадку будь-яке обертання або зміна фази в гільбертовому просторі квантового стану є помилкою, тобто існує нескінченне число різних помилок, які можуть відбутися вже з одним кубітом.

Однак основна й дуже важлива властивість квантового виправлення помилок полягає в тому, що квантовий код, який виправляє деяку дискретну множину помилок, здатний автоматично виправляти безперервну множину помилок [14]. Це відбувається завдяки тому, що вимірювання синдрому помилки або проектує стан з малою помилкою на вихідний стан, тобто стан без помилки, або проектує помилковий стан на один зі станів з дискретної множини великих помилок. Таким чином, відбувається дискретизація квантових помилок, що й дозволяє створити квантові коди для виправлення деякої дискретної множини помилок. Ці коди можуть автоматично виправляти будь-яку помилку в стані квантових систем [14].

Однією з основних моделей квантового шуму є модель деполяризуючого каналу (ДПК) [14]. Для чистого стану окремого кубіту дія цього каналу полягає в наступному: з імовірністю p цей кубіт деполяризується, тобто його стан становиться повністю змішаним, а з імовірністю $(1-p)$ стан кубіту залишається незмінним. Оператор ДПК для кубітів може бути представлений у вигляді [14]:

$$\varepsilon(\rho) = (1-p)\rho + p/3 \cdot \left(\sigma_x \rho \sigma_x + \sigma_y \rho \sigma_y + \sigma_z \rho \sigma_z\right), \tag{4}$$

де ρ – оператор щільності кубіту; σ_x, σ_y та σ_z – оператори Паулі. Таким чином, дія ДПК на кубіт еквівалентна суперпозиції трьох великих дискретних квантових помилок: "класичної" помилки перевороту кубіта, яка описується оператором σ_x, помилки перевороту фази (описується оператором σ_z) та їх комбінації – фазової помилки (описується оператором σ_y). Зрозуміло, що ДПК не описує всі можливі види квантових помилок, але враховує основні види великих дискретних квантових помилок (оскільки помилка загасання фази описується тим же квантовим перетворенням, що і переворот фази, то ДПК враховує і цей вид помилок [14]). Таким чином, ДПК широко використовується у квантовій теорії інформації як модель квантового шуму.

Дія ДПК на окремий кутрит описується більш складним оператором, ніж його дія на кубіт. Згідно з [15],

$$\begin{aligned}\varepsilon_{qutrit}(\rho) = (1-p)\rho + p/8 \cdot \Big(&Y\rho Y^{\dagger} + Z\rho Z^{\dagger} + Y^2\rho\left(Y^2\right)^{\dagger} + YZ\rho(YZ)^{\dagger} + Y^2Z\rho\left(Y^2Z\right)^{\dagger} + \\ &+ YZ^2\rho\left(YZ^2\right)^{\dagger} + Y^2Z^2\rho\left(Y^2Z^2\right)^{\dagger} + Z^2\rho\left(Z^2\right)^{\dagger}\Big),\end{aligned} \tag{5}$$

де $Y = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi i/3} & 0 \\ 1 & 0 & e^{4\pi i/3} \end{pmatrix}$.

Розглянемо тепер режим контролю підслуховування в пінг-понг протоколі з парами переплутаних кутритів для випадку, коли на передаваний кутрит діє оператор шуму (5) (рис. 2). Будемо вважати, що спочатку Єва проводить свою атакуючу операцію, а потім на передаваний кутрит діє оператор шуму, як показано на рис. 2. Згідно зі схемою аналізу загальної некогерентної атаки, яка була запропонована вперше для оригінального протоколу в [2] та узагальнена на протокол з парами кутритів у [8], стани складеної квантової системи "передаваний кутрит – проба Єви" після атаки E можуть бути записані у вигляді:

$$\begin{aligned}\left|\psi^{(0)}\right\rangle &= E\left|0,\varphi\right\rangle = \alpha_0\left|0,\varphi_{00}\right\rangle + \beta_0\left|1,\varphi_{01}\right\rangle + \gamma_0\left|2,\varphi_{02}\right\rangle, \\ \left|\psi^{(1)}\right\rangle &= E\left|1,\varphi\right\rangle = \alpha_1\left|0,\varphi_{10}\right\rangle + \beta_1\left|1,\varphi_{11}\right\rangle + \gamma_1\left|2,\varphi_{12}\right\rangle, \\ \left|\psi^{(2)}\right\rangle &= E\left|2,\varphi\right\rangle = \alpha_2\left|0,\varphi_{20}\right\rangle + \beta_2\left|1,\varphi_{21}\right\rangle + \gamma_2\left|2,\varphi_{22}\right\rangle,\end{aligned} \tag{6}$$

тобто внаслідок повної змішаності стану передаваного кутриту можна умовно вважати, що Боб "посилає" кутрит в одному зі станів $|0\rangle$, $|1\rangle$ або $|2\rangle$ з однаковою ймовірністю 1/3. У формулах (6) $\{|\varphi_{ij}\rangle\}$ ($i, j = 0\ldots2$) – множина станів двокутритної проби Єви.

Матричне представлення атакуючої операції Єви має вигляд:

$$E = \begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ \gamma_0 & \gamma_1 & \gamma_2 \end{pmatrix}. \tag{7}$$

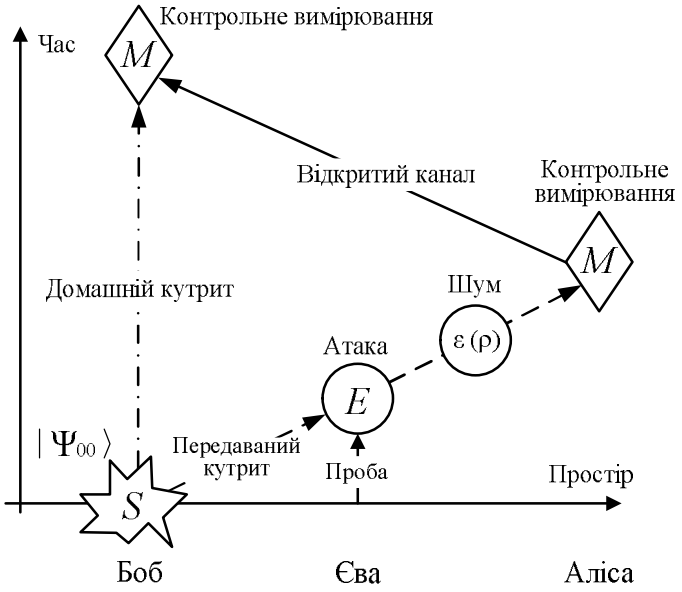


Рис. 2. Режим контролю підслуховування в ДПК при некогерентній атаці

Розглянемо спочатку випадок, коли Боб "посилає $|0\rangle$". Тоді стан передаваного кутриту після переплутуючої операції Єви має вигляд

$$|\psi\rangle = \alpha_0|0\rangle + \beta_0|1\rangle + \gamma_0|2\rangle, \tag{8}$$

а його матриця щільності в базисі $|0\rangle$, $|1\rangle$, $|2\rangle$:

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\beta_0^* & \alpha_0\gamma_0^* \\ \beta_0\alpha_0^* & |\beta_0|^2 & \beta_0\gamma_0^* \\ \gamma_0\alpha_0^* & \gamma_0\beta_0^* & |\gamma_0|^2 \end{pmatrix}. \tag{9}$$

Підставляючи дану матрицю щільності в (5) та виконуючи нескладні, але громіздкі перетворення, в результаті одержимо:

$$\rho_{out} = \frac{1}{8}\begin{pmatrix} \left(3p\left(|\beta|^2 + |\gamma|^2\right) + (8-6p)|\alpha|^2\right) & (8-9p)\alpha\beta^* & (8-9p)\alpha\gamma^* \\ (8-9p)\beta\alpha^* & \left(3p\left(|\alpha|^2 + |\gamma|^2\right) + (8-6p)|\beta|^2\right) & (8-9p)\beta\gamma^* \\ (8-9p)\gamma\alpha^* & (8-9p)\gamma\beta^* & \left(3p\left(|\alpha|^2 + |\beta|^2\right) + (8-6p)|\gamma|^2\right) \end{pmatrix}. \tag{10}$$

Тут і в подальшому індекс "0" у α, β та γ будемо опускати для скорочення запису.

Ймовірність R_z помилкового результату, який свідчить про зміну стану передаваного кутриту, при вимірюванні Боба в z-базисі дорівнює одиниці мінус лівий верхній елемент матриці ρ_{out} (або сумі двох інших діагональних елементів), тобто

$$R_z = 1 - 1/8 \cdot \left(3p\left(|\beta|^2 + |\gamma|^2\right) + (8-6p)|\alpha|^2\right). \tag{11}$$

При реалізації протоколу в ідеальному квантовому каналі ймовірність помилки при вимірюванні Боба в z-базисі, тобто ймовірність виявити атаку Єви, дорівнює [8]:

$$d_z = |\beta|^2 + |\gamma|^2 = 1 - |\alpha|^2. \tag{12}$$

Підставляючи (12) в (11), одержимо

$$R_z = d_z + \frac{3}{4} p\left(1 - \frac{3}{2} d_z\right). \qquad (13)$$

Якщо передаваний кутрит спочатку зазнає дії шуму, а потім свою переплутуючу операцію виконує Єва, то результат (13) не змінюється. Як показують розрахунки, діагональні елементи матриці щільності (10) не залежать від порядку дії операторів атакуючої операції Єви та ДПК.

Розглядаючи тепер випадки, коли Боб "посилає" $|1\rangle$ або $|2\rangle$, що відповідає хвильовим функціям $|\psi^{(1)}\rangle$ та $|\psi^{(2)}\rangle$ в (6), та враховуючи наступні співвідношення між параметрами [8]:

$$|\alpha_0|^2 = |\beta_1|^2 = |\gamma_2|^2; \qquad |\alpha_1|^2 = |\beta_2|^2 = |\gamma_0|^2; \qquad |\alpha_2|^2 = |\beta_0|^2 = |\gamma_1|^2, \qquad (14)$$

для цих випадків одержимо тій же результат (13). Таким чином, повна ймовірність помилки $R_{повна-z}$ при вимірюванні Боба в z-базисі:

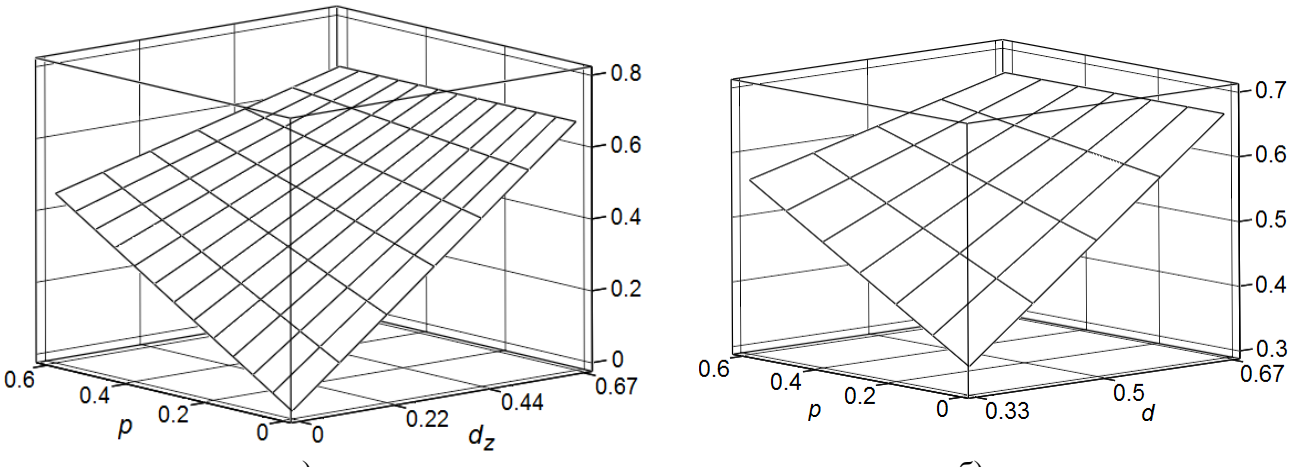
$$R_{повна-z} = \frac{1}{3} \cdot 3R_z = R_z = d_z + \frac{3}{4} \cdot p\left(1 - \frac{3}{2} d_z\right). \qquad (15)$$

Вищенаведені розрахунки можуть бути виконані за аналогією для випадку, коли Боб виконує контрольне вимірювання в базисі x. Ці розрахунки призводять до такого ж за структурою виразу для ймовірність помилки $R_{повна-x}$:

$$R_{повна-x} = d_x + \frac{3}{4} p\left(1 - \frac{3}{2} d_x\right), \qquad (16)$$

де d_x – ймовірність помилки при вимірюванні Боба в x-базисі при реалізації пінг-понг протоколу в ідеальному квантовому каналі.

На рис. 3а наведена залежність $R_{повна-z}$ від d_z та p. Максимальне значення d_z, що відповідає повній інформації Єви, дорівнює 2/3 [8]. Як видно з рис. 3а, суперпозиція операції Єви та шуму в ДПК призводить до того, що при $d_z = 2/3$ $R_{повна-z}$ не залежить від p і також дорівнює 2/3. Таким чином, при некогерентній атаці максимальна імовірність помилки в режимі контролю підслуховування однакова при реалізації протоколу в ідеальному та шумному ДПК.



а) б)

Рис. 3. Залежності повної ймовірності помилки при вимірювані Боба в одному з базисів (а) та середньої ймовірності помилки по двох базисах (б) для ДПК

Відзначимо, що незалежно від рівня помилок d_z, який створює своєю атакою Єва в z-базисі, в x-базисі вона створює максимальний рівень $d_x = 2/3$, та навпаки [8]. На рис. 3б показана залежність

$$R_{повна} = 1/2 \cdot (2/3 + R_{повна-z}) \qquad (17)$$

від p та середнього рівня помилок, створюваних атакою, по обох базисах: $d = 1/2 \cdot (2/3 + d_z)$, – при умові, що легітимні користувачі перемикаються між z- та x-базисами з однаковою ймовірністю 1/2, що є для них найбільш розумною стратегією контролю підслуховування [8].

3. Імітаційна модель пінг-понг протоколу з парами кутритів у квантовому каналі з шумом

В даній моделі імітується робота пінг-понг протоколу з парами кутритів у ДПК при наявності атаки Єви. В режимі контролю підслуховування збирались статистичні дані щодо рівня помилок у *x*-, *z*- базисах та їх середні значень. Ці статистичні дані використовувались для отримання практичних рекомендацій щодо використання пінг-понг протоколу в квантовому каналі з шумом.

Крім того, в даній моделі використовувався неквантовий спосіб підсилення безпеки пінг-понг протоколу, який детально описаний в роботі [13]. Наведемо його короткий опис. Перед початком передачі Аліса розбиває своє трійкове повідомлення на l блоків $a_i (i = 1 \ldots l)$ деякої фіксованої довжини r, після чого для кожного блоку окремо генерує випадкову, оборотну над полем Галуа GF(3) (оборотну трійкову) матрицю M_i розміром $r \times r$ й множить отримані матриці на відповідні блоки повідомлення:

$$b_i = M_i a_i . \tag{18}$$

Отримані в результаті блоки передаються квантовим каналом з використанням пінг-понг протоколу. Навіть якщо Єві вдасться перехопити один (або декілька) із цих блоків, залишившись невиявленою, то, не знаючи використаних матриць M_i, Єва не зможе відновити вихідні блоки a_i. Матриці M_i передаються Бобові через звичайний відкритий канал після завершення квантового передавання, але тільки в тому випадку, якщо Аліса й Боб переконалися у відсутності підслуховування в квантовому каналі. Потім Боб обертає отримані матриці та, помноживши їх на відповідні блоки b_i, відновлює вихідні блоки:

$$a_i = M_i^{-1} b_i . \tag{19}$$

Для забезпечення високого рівня стійкості довжина блока *r* і відповідний розмір матриць M_i $(r \times r)$ обирався так, щоб імовірність успішної атаки Єви *s* після передачі одного блока була нехтовно малою величиною. Ця імовірність *s* обчислюється за формулою $s(I,q,d) = \left(\frac{1-q}{1-q\cdot(1-d)} \right)^{I/I_0}$, де I – кількість інформації, що отримує Єва при передаванні одного блока, I_0 – кількість інформації Єви за один цикл режиму передавання повідомлення, q – імовірність переходу в режим контролю підслуховування [13]. Вважаючи $s(I,q,d) = 10^{-k}$, одержуємо формулу обрахунку кількості інформації Єви I і обираємо довжину блока *r*:

$$r \geq I = -kI_0 / \lg((1-q)/(1-q\cdot(1-d))) . \tag{20}$$

При моделювання пінг-понг протоколу з парами кутритів використовувались такі вхідні параметри: 1) `length = 10000 трит` – довжина передаваних трійкових даних; 2) $k = 4$ – показник степені десятки для обрахунку ймовірності невиявлення атаки Єви, тобто $s(I,q,d) = 10^{-k}$; 3) q = 0,1 … 0,5 – імовірність перемикання протоколу в режим контролю підслуховування та $(1-q)$ – імовірності перемикання в режим передавання повідомлення; 4) Для розрахунку величини *r* (20) бралось: $I_0 = 2$ – кількість інформації, яку отримає Єва за один раунд (припускали для надійності, що Єва отримує повну інформацію за один раунд, тобто 2 трити), $d = 1/3$ – рівень помилок, що створює Єва (припускали, що Єва створює мінімально можливий рівень помилок, див. [13]); 5) $d_x = 0 \ldots 2/3$ – імовірність виявлення атаки при вимірюванні в *x*-базисі (при реалізації пінг-понг протоколу в ідеальному квантовому каналі); 6) $d_z = 2/3$ – імовірність виявлення атаки при вимірюванні в *z*-базисі (в одному з базисів імовірність виявлення атаки завжди максимальна та не залежить від імовірності виявлення атаки в другому базисі [8]); 7) p = 0 … 0,5 – імовірність деполяризації стану кубіту та $(1-p)$ – імовірність незмінності стану кубіту (див. (5)); 8) $q_x = q_z = 0{,}5$ – імовірність перемикання легітимними користувачами між *z*- та *x*-базисами (вважали, що $q_x = q_z$ – є найбільш розумною стратегією контролю підслуховування).

Параметри *length*, q, d_x та p фіксувались на початку моделювання, після чого виконувались наступні операції: **1.** Спочатку розраховувалась величина d_{Eva} (середня по двох базисах імовірність виявлення атаки в ідеальному каналі) за формулою $d_{Eva} = q_z d_z + q_x d_x$. Ця величина показує середній рівень помилок, який буде реєструватись в режимі контролю підслуховування в ідеальному каналі і необхідна для порівняння з відповідною величиною в шумному каналі $R_{повна}$ (17), яка враховує одночасну зміну станів передаваних фотонів внаслідок операцій Єви та природного шуму. **2.** Розраховувалась довжина блоку даних *r* (20) та кількість самих блоків *l*, на які розіб'ються передавані дані. Величина *l* вираховувалась за формулою $l = lenght/r$. **3.** Розраховувались параметри Err_x, Err_z, Err_{mean} (імовірності помилки при вимірюванні в *x*-базисі, *z*-базисі та середнє значення по двох базисах, див. (15) – (17)), за формулами:

$$Err_x = d_x + 3/4 \cdot p \cdot (1 - 3/2 \cdot d_x),\ Err_z = d_z + 3/4 \cdot p \cdot (1 - 3/2 \cdot d_z),\ Err_{mean} = q_x \cdot Err_x + q_z \cdot Err_z. \quad (21)$$

4. Генерувались псевдовипадкові трійкові вихідні дані розміром *length* (імовірність генерації "0", "1", "2" бралась рівною 1/3). **5.** Згенеровані в пункті 4 псевдовипадкові трійкові дані розбивались на *l* менших блоків $a_i (i = 1 \ldots l)$ розміром *r* (останній блок при необхідності доповнювався до розміру *r* випадковими тритами), де над ними виконувались наступні операції: **5.1.** Для кожного блоку a_i генерувалась випадкова, оборотна над полем GF(3) матриця M_i розміром $r \times r$. **5.2.** Виконувалось перемноження $M_i a_i$ в полі Галуа GF(3), в результаті отримували b_i (18). **5.3.** Далі виконувалась передача b_i за допомогою пінг-понг протоколу в квантовому каналі з шумом. З ймовірностями q та $(1-q)$ відбувалось перемикання в режим контролю підслуховування або в режим передавання повідомлення відповідно. В режимі передавання повідомлення Боб приймав пару кутритів через квантовий канал (в цьому режимі помилки, обумовлені як атакою Єви, так і шумом в каналі, не моделювались). В режимі контролю підслуховування з ймовірностями $q_x = q_z = 1/2$ обирався відповідний базис та фіксувалась загальна кількість переходів в цей базис (Kp_x, Kp_z), і в ньому з імовірністю Err_x для *x*-базису (Err_z – для *z*-базису) моделювалась помилка та рахувалась кількість помилок Co_{Dx} (Co_{Dz}). Перемикання між режимами відбувалось доти, поки не передасться повністю блок b_i. **5.4.** Для кожного переданого блоку b_i обраховувались $b_i\_Errlvl_x$, $b_i\_Errlvl_z$ та $b_i\_Errlvl_{mean}$ (середній рівень помилок в базисі *x*, середній рівень помилок в базисі *z* та середній рівень помилок по двох базисах відповідно) за формулами:

$$b_i\_Errlvl_x = Co_{Dx}/Kp_x,\ b_i\_Errlvl_z = Co_{Dz}/Kp_z,\ b_i\_Errlvl_{mean} = (Co_{Dx} + Co_{Dz})/(Kp_x + Kp_z). \quad (22)$$

6. На основі зібраної статистики обраховувались отримані при моделюванні мінімальні ($MinErrlvl_x$, $MinErrlvl_z$, $MinErrlvl$) та максимальні ($MaxErrlvl_x$, $MaxErrlvl_z$, $MaxErrlvl$) рівні помилок, а також середні по всіх *l* переданих блоках ($MeanErrlvl_x$, $MeanErrlvl_z$, *MeanErrlvl*).

Результати моделювання наведені в табл. 1. Як видно, середні значення рівня помилок по всіх переданих блоках *MeanErrlvl* в межах статистичної похибки дорівнюють відповідним теоретичним значенням Err_{mean}, отриманим за формулою (21). Але такий результат виходить за умови достатньо великого числа переданих блоків. У той же час, мінімальні рівні помилок навіть по обох базисах (*MinErrlvl*) є достатньо малими та в більшості випадків меншими за рівень природного шуму *p*, особливо при великих *p* (див. табл. 1). Цей факт є наслідком випадкової природи квантових вимірювань. Таким чином, передавши один блок та перевіривши рівень помилок у режимі контролю підслуховування, Аліса та Боб можуть зробити помилковий висновок, що підслуховування немає. Тому в шумному каналі, і особливо при достатньо високому рівні природних шумів, легітимні користувачі повинні передати достатньо велику кількість гешованих блоків, як мінімум декілька десятків, і тільки потім прийняти рішення про наявність або відсутність атаки Єви (і відповідно про

необхідність або перервати протокол, або передати геш-матриці від Аліси до Боба). В цьому і полягає основна рекомендація щодо практичної реалізації пінг-понг протоколу з переплутаними парами кутритів в ДПК.

Як показують результати моделювання, середні рівні помилок практично не залежать від імовірності переключення в режим контролю підслуховування q (див. табл. 1). Але від цієї ймовірності суттєво залежить швидкість передавання даних пінг-понг протоколом: чим менше q, тим частіше передаються дані й тим вище швидкість. Але від q суттєво залежить і довжина блоку r – вона збільшується зі зменшенням q відповідно до експоненційного закону [16]. Відповідно, збільшується і розмір оборотних геш-матриць. Тому, зменшуючи q, легітимні користувачі повинні будуть витрачати більше часу на генерацію оборотних матриць. Але, враховуючи достатньо високий реальний рівень завад при передаванні фотонів квантовим каналом, цей час, ймовірно, буде скомпенсований за рахунок підвищення швидкості пінг-понг протоколу при зменшенні q.

Відзначимо також, що при $p = 0{,}5$ та атаці Єви, при якій вона прагне створити нульовий рівень помилок в одному з базисів (наприклад, $d_x = 0$, $d_{Eva} = 0{,}333$), середній рівень помилок *MeanErrlvl* майже не перевищує p, тому легітимні користувачі знову таки можуть зробити помилковий висновок про відсутність атаки. Але в цьому випадку вони повинні перевірити середній рівень помилок в кожному з базисів x та z окремо – в одному з цих базисів рівень помилок буде близький до $2/3$. Також можна зробити висновок, що легітимні користувачі для надійного детектування атаки повинні використовувати квантовий канал з природним рівнем шумів $p \le 0{,}5$, на практиці це означає використання каналу обмеженої довжини.

Висновки. У даній роботі розроблено модель режиму контролю підслуховування для пінг-понг протоколу з парами кутритів у каналі з шумом та проведено імітаційне моделювання роботи даного протоколу в шумному каналі. Отримано формулу для повної ймовірності помилкового результату при вимірювані в режимі контролю підслуховування. Показано, що максимальна імовірність помилки в режимі контролю підслуховування однакова при реалізації протоколу в ідеальному та шумному ДПК. Встановлено, що в ДПК, і особливо при достатньо високому рівні шумів, легітимні користувачі повинні передати достатньо велику кількість блоків інформації (як мінімум декілька десятків) і тільки потім прийняти рішення про наявність або відсутність атаки. Також встановлено, що легітимні користувачі для надійного детектування атаки на практиці повинні використовувати квантовий канал обмеженої довжини з природним рівнем шумів $p \le 0{,}5$.

Таблиця 1. Результати моделювання

d			d_x= 0; d_z= 0,667; d_{Eva}= 0,333			d_x= 0,333; d_z= 0,667; d_{Eva}= 0,5			d_x= 0,667; d_z= 0,667; d_{Eva}= 0,667		
p			**p=0,1**	**p=0,3**	**p=0,5**	**p=0,1**	**p=0,3**	**p=0,5**	**p=0,1**	**p=0,3**	**p=0,5**
Errx			0,075	0,225	0,375	0,371	0,446	0,521	0,667	0,667	0,667
Errz			0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667	0,667
Errmean			0,371	0,446	0,521	0,519	0,556	0,594	0,667	0,667	0,667
$k = 4$; *length* = 10000	$q = 0{,}5$; $r = 66$; $l = 152$	*MinErrlvlx*	0,000	0,000	0,100	0,091	0,111	0,167	0,263	0,333	0,350
		MinErrlvlz	0,308	0,368	0,333	0,300	0,364	0,300	0,333	0,333	0,143
		MinErrlvl	**0,138**	**0,250**	**0,300**	**0,261**	**0,278**	**0,368**	**0,395**	**0,450**	**0,444**
		MaxErrlvlx	0,312	0,526	0,714	0,692	0,813	0,857	0,938	1,000	0,929
		MaxErrlvlz	1,000	1,000	1,000	1,000	0,917	0,941	0,875	1,000	1,000
		MaxErrlvl	0,640	0,632	0,882	0,700	0,865	0,810	0,857	0,862	0,955
		MeanErrlvlx	0,086	0,228	0,375	0,350	0,437	0,545	0,661	0,667	0,672
		MeanErrlvlz	0,665	0,658	0,658	0,673	0,654	0,669	0,662	0,675	0,667
		MeanErrlvl	**0,387**	**0,446**	**0,516**	**0,510**	**0,547**	**0,607**	**0,661**	**0,672**	**0,669**
	q = 0,25;	*MinErrlvlx*	0,000	0,000	0,100	0,091	0,143	0,000	0,400	0,400	0,357
		MinErrlvlz	0,333	0,400	0,364	0,412	0,412	0,333	0,333	0,429	0,200
		MinErrlvl	**0,136**	**0,261**	**0,318**	**0,316**	**0,400**	**0,382**	**0,464**	**0,483**	**0,429**

		MaxErrlvlx	0,333	0,500	0,600	0,700	0,750	0,857	0,929	1,000	0,923
		MaxErrlvlz	0,929	0,929	1,000	0,889	1,000	0,938	1,000	0,875	1,000
		MaxErrlvl	0,619	0,684	0,692	0,741	0,769	0,744	0,905	0,900	0,92
		MeanErrlvlx	0,074	0,235	0,369	0,376	0,472	0,501	0,686	0,685	0,644
		MeanErrlvlz	0,659	0,661	0,665	0,663	0,675	0,650	0,671	0,682	0,692
		MeanErrlvl	**0,369**	**0,446**	**0,513**	**0,522**	**0,577**	**0,583**	**0,678**	**0,684**	**0,671**
	$q = 0,1; r = 508; l = 20$	*MinErrlvlx*	0,000	0,000	0,200	0,143	0,250	0,273	0,417	0,500	0,500
		MinErrlvlz	0,412	0,364	0,273	0,353	0,435	0,375	0,333	0,385	0,300
		MinErrlvl	**0,175**	**0,250**	**0,368**	**0,258**	**0,412**	**0,394**	**0,517**	**0,500**	**0,500**
		MaxErrlvlx	0,250	0,500	0,588	0,600	0,625	0,700	0,857	0,941	0,800
		MaxErrlvlz	0,900	0,867	0,818	0,909	0,846	0,846	0,875	0,909	0,889
		MaxErrlvl	0,704	0,588	0,667	0,680	0,704	0,750	0,808	0,833	0,793
		MeanErrlvlx	0,078	0,234	0,418	0,355	0,451	0,533	0,671	0,669	0,678
		MeanErrlvlz	0,676	0,637	0,630	0,644	0,672	0,661	0,637	0,651	0,634
		MeanErrlvl	**0,367**	**0,437**	**0,538**	**0,500**	**0,551**	**0,589**	**0,658**	**0,660**	**0,653**

У подальшому можливе удосконалення запропонованої моделі шляхом врахування помилок у режимі передачі повідомлення й використання завадостійких кодів для кутритів.

Список літератури

1. *Баумейстер Д.* Физика квантовой информации / Д. Баумейстер, А. Экерт, А. Цайлингер. – М. : "Постмаркет", 2002. – 376 с.
2. *Bostrom K.* Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, issue 18. – 187902.
3. *Cai Q.-Y.* Improving the capacity of the Bostrom – Felbinger protocol / Q.– Y. Cai, B.– W. Li // Physical Review A. – 2004. – V. 69, issue 5. – 054301.
4. *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.
5. *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.
6. *Wang Ch.* Quantum secure direct communication with high dimension quantum superdense coding / Ch. Wang, F.-G. Deng, Y.-S. Li [et al] // Physical Review A. – 2005. – V. 71, issue 4. – 044305.
7. *Васіліу Є.В.* Пінг–понг протокол з повністю переплутаними станами пар та триплетів тривимірних квантових систем / Є.В. Васіліу // Цифрові технології. – 2009, № 5. – С. 18–26.
8. *Василиу Е.В.* Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов / Е.В. Василиу, Р.С. Мамедов // Восточноевропейский журнал передовых технологий. – 2009, № 4/2 (40). – С. 4–11.
9. *Zhang Zh.-J.* Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss / Zh.-J. Zhang, Y. Li, Zh.-X. Man // Physics Letters A. – 2005. – V. 341, issue 5–6. – P. 385–389.
10. *Cai Q.-Y.* The "Ping-pong" protocol can be attacked without eavesdropping / Q.-Y. Cai // Physical Review Letters. – 2003. – V. 91, issue 10. – 109801.
11. *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.
12. *Василиу Е.В.* Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем / Е.В. Василиу // Информатика: Объединенный институт проблем информатики НАН Беларуси. – 2009, № 1 (21) – С. 117–128.
13. *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.
14. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. – М. : Мир, 2006. – 824 с.
15. *Ramzan M.* Noisy non-transitive quantum games / M. Ramzan, S. Khan, M.K. Khan // J. Phys. A: Math. Theor. – 2010. – V. 43, N. 26. – 265304.
16. *Василиу Е.В.* Оценки вычислительной сложности неквантового способа усиления безопасности пинг-понг протокола / Е.В. Василиу // Прикладная радиоэлектроника. – 2009, № 3. – С. 396–404.

Рецензент: д.т.н., проф. Дудикевич В.Б.
Надійшла 17.02.2010 р.