УДК003.26:621.39+530.145 **Васіліу Є.В.**

ЕТАПИ СТРУКТУРНОГО СИНТЕЗУ КВАНТОВИХ СИСТЕМ ПРЯМОГО БЕЗПЕЧНОГО ЗВ'ЯЗКУ

В роботі розглядаються етапи синтезу структури квантових систем прямого безпечного зв'язку, які ґрунтуються на різних варіантах пінг-понг протоколу. Детально описані схеми цих етапів за публікаціями автора та інших фахівців. Зокрема, показано, що доповнюючи пінг-понг протокол процедурою підсилення стійкості, можливо синтезувати квантову систему прямого безпечного зв'язку з заданим рівнем стійкості до атаки пасивного перехоплення.

Ключові слова: квантова система, криптографія, пінг-понг протокол, інформація, атака пасивного перехоплення.

Методи квантової криптографії швидко розвиваються протягом останніх двох десятиріч. На основі цих методів пропонуються нові підходи до побудови захищених систем конфіденційного зв'язку. Робота таких систем, які ґрунтуються на протоколах квантової криптографії, потребує використання не тільки самих цих 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. На даний час запропоновані різні види квантових протоколів прямого безпечного зв'язку. Більшість з них потребує передачі кубітів блоками. Це дозволяє виявити прослуховування квантового каналу до початку передавання самого повідомлення й таким способом гарантувати безпеку передачі – якщо прослуховування виявлене до передавання повідомлення, то легітимні користувачі (Аліса та Боб) переривають сеанс і ніяка інформація не попадає до зловмисника (Єви). Але для зберігання таких блоків кубітів необхідна квантова пам'ять великого обсягу. Технологія квантової пам'яті активно розробляється, але ця технологія поки ще далека від масового застосування в стандартному телекомунікаційному устаткуванні. Тому з погляду технічної реалізації перевагу мають протоколи, у яких передавання здійснюється одиночними кубітами або невеликими їх групами (за один цикл протоколу). Одним з таких протоколів є так званий пінг-понг протокол [3], який не потребує для своєї практичної реалізації великої квантової пам'яті і може виконуватися з використанням існуючого технічного обладнання [4].

У початковому варіанті пінг-понг протоколу використовуються два стани Бела переплутаної пари кубітів, що дозволяє передати один біт класичної інформації за один цикл протоколу [3]. Використання всіх чотирьох белівських станів пари кубітів, тобто квантового надщільного кодування, дозволяє передати два біти за цикл [5]. Подальше збільшення інформаційної місткості можливе при використанні замість переплутаних пар кубітів їх трійок, четвірок і т.д. [6]. Інший шлях підвищення інформаційної місткості пінг-понг протоколу – це використання переплутаних станів багаторівневих квантових систем. Так, пінг-понг протокол з використанням переплутаних станів пар та триплетів три-рівневих систем (кутритів) та квантового надщільного кодування для кутритів розроблений у [7,8].

Різні атаки, як на оригінальний пінг-понг протокол, так і на його вдосконалені варіанти, були розглянуті в ряді робіт [2,3,9–12]. У роботі [2] запропонований неквантовий спосіб підсилення безпеки пінг-понг протоколу, який полягає в оборотному гешуванні бітових блоків повідомлення множенням їх на випадкові оборотні матриці. Також запропоновано

використовувати для пінг-понг протоколу в квантовому каналі з завадами класичний завадостійкий код, що виправляє пакети помилок [13]. Таким чином, розробка нового квантового протоколу безпечного зв'язку (або вдосконалення за якимись параметрами вже запропонованого), обчислення рівня його стійкості до різних видів атак, розробка процедур підвищення стійкості та побудова завадостійких кодів з урахуванням особливостей передавання інформації в даному протоколі є етапами синтезу структури квантової системи прямого безпечного зв'язку. *Метою* цієї роботи є розробка підходу до проблеми структурного синтезу квантових систем прямого безпечного зв'язку, що базуються на пінг-понг протоколі, а також детальний опис відповідних етапів.

Розробка нового квантового протоколу прямого безпечного зв'язку. Оскільки квантовий прямий безпечний зв'язок призначений для прямого, тобто без використання шифрування, передавання секретних повідомлень, то створення нового протоколу необхідно розпочати з розробки схеми квантового кодування інформації. Розглянемо цей етап синтезу квантової системи безпечного зв'язку на прикладі пінг-понг протоколу. В цьому протоколі використовують переплутані стани кубітів або багаторівневих квантових систем. Ідея кодування полягає в тому, що кожній групі класичних бітів (для протоколу з кубітами) 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. Наприклад, існує вісім ортогональних три-кубітних станів Грінбергера – Хорна – Цайлінгера (ГХЦ), що дозволяє кодувати одним станом три класичних біти, а крім цього, використовувати квантове надщільне кодування, тобто передавати три класичних біти, передаючи квантовим каналом два кубіти. Квантове надщільне кодування дозволяє зменшити рівень помилок при передаванні в реальному квантовому каналі за рахунок зменшення кількості кубітів, що передаються. В табл. 1 наведена для прикладу схема квантового кодування для пінг-понг протоколу з ГХЦ-триплетами [6]. В цей табл. I – тотожній оператор, σ_x, σ_y, та σ_z – оператори Паулі.

Схема квантового кодування для пінг-понг протоколу з ГХЦ-триплетами Таблиця 1

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

Аналогічні схеми кодування розроблені для пінг-понг протоколів з переплутаними ГХЦ- та кластерними станами четвірок кубітів [6,14], а також з парами та трійками кутритів [7,8]. Відзначимо, що пошук сімейств переплутаних ортогональних станів трьох і більшого числа кубітів (а також багаторівневих квантових систем) є окремою проблемою квантової фізики. Існує багато публікацій, в яких знайдено такі сімейства, і для розробки нового варіанта протоколу квантового безпечного зв'язку можна скористатися результатами цих робіт. Підкреслимо також, що описаний метод розробки схеми квантового кодування придатний для створення будь-якого протоколу, що ґрунтується на використанні властивостей переплутаних станів, зокрема не тільки для різних варіантів пінг-понг протоколу, а і для протоколів з передаванням кубітів блоками.

Наступний етап створення квантового протоколу безпечного зв'язку полягає в розробці методів виявлення різних атак на протокол та методів протидії цим атакам. Так, для пінг-понг протоколу на сьогодні відомо декілька атак, серед яких атака пасивного перехоплення (підслуховування) в ідеальному та шумному квантовому каналі, атака «відмова в обслуговуванні», атака «людина посередині» тощо [9,11]. Існують і методи протидії цим атакам. Так, наприклад, атака «людина посередині» буде неможливою, якщо легітимні сторони супроводжують кодом автентифікації всі повідомлення, що передаються класичним каналом зв'язку. Основну загрозу для протоколів квантового прямого безпечного зв'язку являє атака пасивного перехоплення, яку б не могли виявити легітимні користувачі. Тому розробка схеми контролю підслуховування в квантовому каналі є першочерговим завданням при розробці нового протоколу. Основна ідея методу контролю підслуховування полягає у використанні властивостей переплутаних станів, які розділюють легітимні сторони. Одна зі схем, що дозволяє використати ці властивості, полягає в наступному. Одна з легітимних сторін, наприклад Аліса, вимірює послідовно стани кубітів, які заходяться у неї, в одночастковому базисі, а потім таку ж серію вимірювань виконує Боб (або навпаки). При цьому потрібно використовувати *два* неортогональних базиси, перемикаючись між ними випадковим чином. Вимірювання стану, як мінімум, останнього кубіта дає певний результат з імовірністю, що дорівнює одиниці. Якщо ж стан було збурено в процесі передавання кубітів, тобто Боб не отримує очікуваного результату, то це є свідченням або підслуховування, або природних завад у квантовому каналі. Але при використанні сучасного обладнання середній рівень помилок при передаванні кубітів квантовим каналом дорівнює декільком відсоткам [4]. Підслуховування в пінг-понг протоколі створює значно більший рівень помилок [2,3,12], що дозволить легітимним користувачам виявити його з високою ймовірністю. Схема контролю підслуховування для оригінального пінг-понг протоколу була розроблена в [3]. Декілька схем контролю підслуховування для протоколів з передаванням кубітів блоками також розроблено в ряді робіт, наприклад [7,10,15]. На основі цих схем автором даної статті розроблено схеми контролю підслуховування для декількох варіантів пінг-понг протоколу [6,8,14]. На рис. 1 дано графічну ілюстрацію режиму передавання повідомлення та режиму контролю підслуховування для пінг-понг протоколу з ГХЦ-триплетами [11]. Аліса та Боб перемикаються між цими режимами з імовірністю q. В табл. 2 показана схема вимірювань для контролю підслуховування в протоколі з ГХЦ-триплетами [6,11]. Відзначимо, що ця схема трохи відрізняється від описаної вище – тут при виборі Бобом базису σ_x Аліса виконує вимірювання у двочастковому базисі Бела.

Схема вимірювань для контролю підслуховування в протоколі з ГХЦ-триплетами — Таблиця 2

Базис σ_z		Базис σ_x	
Результат Боба	Результати Аліси	Результат Боба	Результат Аліси
кубіт 3	кубіти 1,2	кубіт 3	кубіти 1,2
$\|0\rangle$	$\|0\rangle$, $\|0\rangle$	$\|+\rangle$	$\|\Psi^+\rangle = (\|00\rangle + \|11\rangle)/\sqrt{2}$
$\|1\rangle$	$\|1\rangle$, $\|1\rangle$	$\|-\rangle$	$\|\Psi^-\rangle = (\|00\rangle - \|11\rangle)/\sqrt{2}$

Обчислення рівня стійкості протоколу до атаки пасивного перехоплення. Як відзначено вище, атака пасивного перехоплення інформації є однією з основних атак на

протоколи квантового прямого безпечного зв'язку. Схема такої атаки на оригінальний пінг-понг протокол та схема аналізу цієї атаки були розроблені в [3]. Згодом на основі ідей роботи [3] виконано аналіз атаки пасивного перехоплення на пінг-понг протокол з ГХЦ-триплетами [11] та отримані результати узагальнено на протокол з n-кубітними ГХЦ-станами для довільних n [2]. Також виконано аналіз цієї атаки на пінг-понг протокол з чотири-кубітними кластерними станами та протокол з белівськими станами пар кутритів [12].

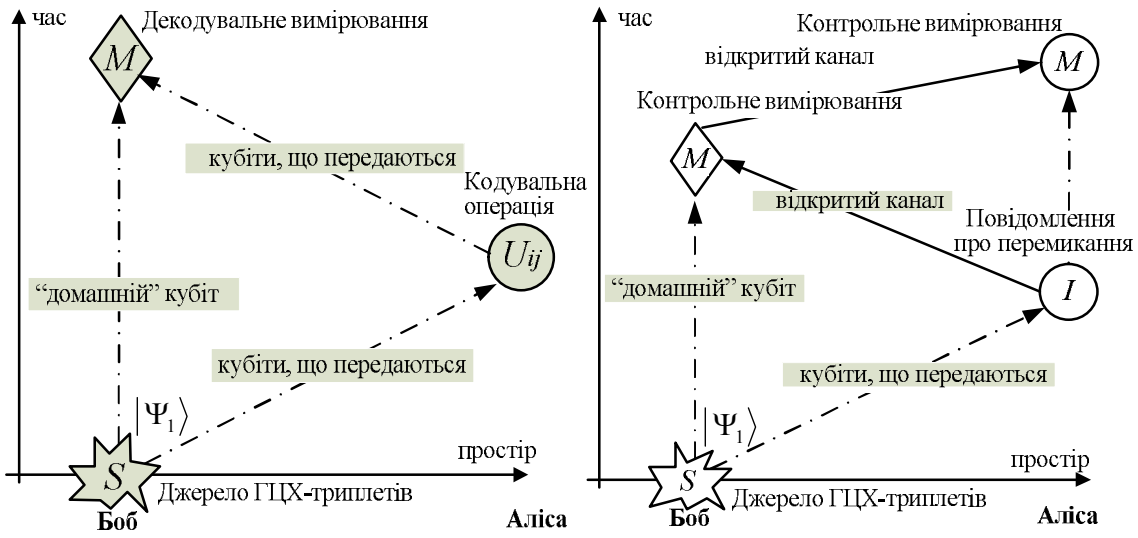

Рис. 1. Режим передавання повідомлення (а)
та режим контролю підслуховування (б)
для протоколу з ГХЦ-триплетами

На рис. 2 показана схема атаки пасивного перехоплення на пінг-понг протокол з ГХЦ-триплетами [11]. Єва переплутує свою допоміжну квантову систему – пробу (зонд) з передаваними кубітами на шляху Боб $\rightarrow$ Аліса, а потім виконує вимірювання над складеною квантовою системою "передавані кубіти – проба" на шляху Аліса $\rightarrow$ Боб. При цьому стан ГХЦ-триплета збурюється, що можуть виявити легітимні користувачі у режимі контролю підслуховування. Аналогічний вид мають схеми цієї атаки на інші варіанти пінг-понг протоколу [12].

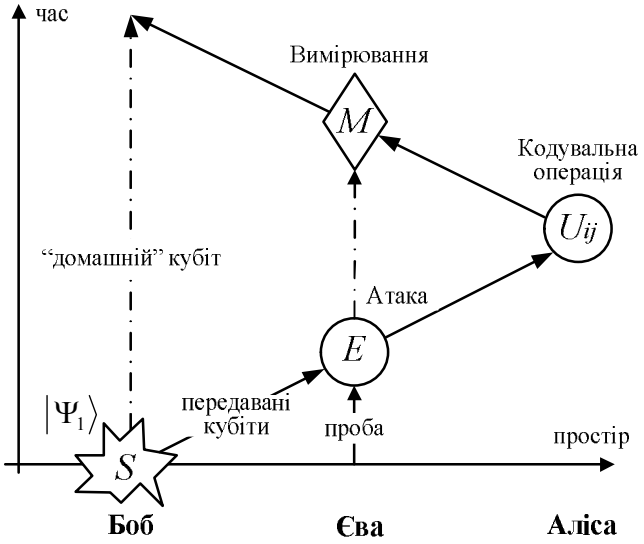

Рис. 2. Схема атаки пасивного перехоплення на протокол з ГХЦ-триплетами

Коротко, схема аналізу атаки пасивного перехоплення на пінг-понг протокол є такою. Кількість інформації Єви при атаці на один цикл протоколу визначається ентропією фон Неймана:

$$I_0 = S(\rho) \equiv -Tr \{ \rho \log_2 \rho \} = -\sum_i \lambda_i \log_2 \lambda_i , \quad (1)$$

де λ_i – власні значення матриці щільності ρ системи "передавані кубіти – проба Єви".

Далі необхідно виписати матрицю щільності ρ для конкретного варіанта пінг-понг протоколу й знайти її власні значення, як функції від імовірності виявити атаку d при однократному переході в режим контролю підслуховування. Таким чином виходить формула для кількості інформації (1) як функція від d. Для пінг-понг протоколу з n-кубітними ГХЦ-станами цю формулу можна отримати у явному вигляді [2]. Для протоколу з чотири-кубітними кластерними станами та протоколу з парами кутритів можна отримати алгебраїчні рівняння четвертого та третього степеня відповідно для знаходження λ_i. Розв'язуючи чисельно ці рівняння й підставляючи результати в (1), також отримуємо залежність $I_0(d)$ у числовому вигляді. Ми не наводимо тут всі ці формули та рівняння через їхню громіздкість (див. [2,3,11,12]).

Імовірність того, що Єва не буде виявлена після m успішних атак і одержить інформацію $I = mI_0$, визначається виразом [3]:

$$s(I,q,d) = \left(\frac{1-q}{1-q(1-d)} \right)^{\frac{I}{I_0}}, \quad (2)$$

На рис. 3 у логарифмічному масштабі наведені залежності s від I при q=0.5 та значенні d, яке відповідає максимальній інформації Єви. При цьому I_0 (1) розраховувалась при однакових значеннях частот кодувальних операцій Аліси. В усіх варіантах пінг-понг протоколу, крім оригінального протоколу [3], використовується квантове надщільне кодування для збільшення інформаційної місткості протоколу.

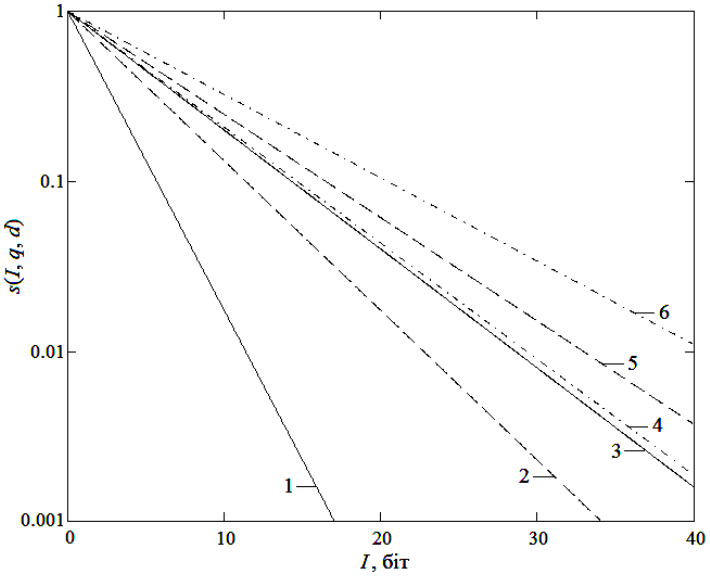

Рис. 3. Повна ймовірність невиявлення атаки s для різних варіантів пінг-понг протоколу:
1 – оригінальний протокол; 2 – протокол з белівськими станами пар кубітів;
3 – протокол з белівськими станами пар кутритів; 4 – протокол з ГХЦ-четвірками кубітів;
5 – протокол з чотири-кубітними кластерними станами; 6 – протокол з ГХЦ-шестірками кубітів

В табл. 3 наведена інформаційна місткість (на один раунд) тих варіантів пінг-понг протоколу, рівень стійкості яких до атаки пасивного перехоплення показаний на рис. 3.

Також приведені значення максимальних ймовірностей виявлення атаки за один раунд контролю підслуховування $d_{\max}$, при яких інформація Єви максимальна.

Інформаційна місткість різних варіантів пінг-понг протоколу Таблиця 3

Варіант пінг-понг протоколу	Інформаційна місткість, біт	$d_{\max}$
оригінальний протокол без надщільного кодування	1	0.5
протокол з белівськими станами пар кубітів	2	0.5
протокол з белівськими станами пар кутритів	$\log_2 9 \approx 3.17$	2/3
протокол з ГХЦ-четвірками кубітів	4	0.875
протокол з чотири-кубітними кластерними станами	4	0.75
протокол з ГХЦ-шестірками кубітів	6	0.9688

Як видно з рис. 3, всі варіанти пінг-понг протоколу мають *асимптотичну* стійкість до атаки пасивного перехоплення, тобто атака буде виявлена, але Єва зможе перехопити деяку (невелику) кількість інформації. При цьому з рис. 3 та табл. 3 випливає також, що інформаційна місткість та асимптотична стійкість різних варіантів пінг-понг протоколу знаходяться в обернено пропорційній залежності. Логарифмуючи вираз (2), можна знайти кількість інформації *I*, яка утече до Єви при заданій повній імовірності невиявлення атаки *s*. У табл. 4 наведені округлені (у більшу сторону) значення *I* при $s = 10^{-4}$ та $d = d_{\max}$; q – ймовірність переходу у режим контролю підслуховування.

Кількість інформації, що утікає до Єви, при $s = 10^{-4}$, біт Таблиця 4

Варіант пінг-понг протоколу	q = 0,5	q = 0,25
оригінальний протокол без надщільного кодування	23	60
протокол з белівськими станами пар кубітів	46	120
протокол з белівськими станами пар кутритів	58	146
протокол з ГХЦ-четвірками кубітів	59	144
протокол з чотири-кубітними кластерними станами	66	166
протокол з ГХЦ-шестірками кубітів	82	198

Так як всі варіанти пінг-понг протоколу мають асимптотичну стійкість до атаки пасивного перехоплення, то звідси витікає, що необхідним є ще один структурний елемент квантової системи безпечного зв'язку – процедура підсилення стійкості протоколу. Як відзначено вище, пінг-понг протокол уразливий, крім атаки пасивного перехоплення, і до деяких інших видів атак. Але методи захисту проти цих атак також розроблені. В даній роботі ці атаки та методи захисту від них не розглядаються (див., наприклад, [11]). Але аналіз таких атак та розробка методів захисту проти них також є елементами синтезу структури квантових систем прямого безпечного зв'язку, що ґрунтуються на пінг-понг протоколі.

Процедура підсилення стійкості пінг-понг протоколу. Ця процедура вперше була запропонована в [2]. Наведемо її короткий опис. Перед початком передачі Аліса розбиває своє двійкове повідомлення (або трійкове для протоколу з кутритами) на *l* блоків деякої фіксованої довжини *r*, позначимо ці блоки через a_i $(i = 1,\ldots l)$. Потім Аліса генерує для кожного блока *окремо* випадкову, оборотну над полем Галуа GF(2) (або GF(3) для протоколу з кутритами) матрицю M_i розміру $r \times r$ і множить отримані матриці на відповідні блоки повідомлення:

$$b_i = M_i a_i . \qquad (3)$$

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. Очевидно, що атака прямого перебору матриць стає абсолютно нездійсненною (при поточному рівні швидкодії обчислювальної техніки) вже при їхньому розмірі порядку 16×16, тому що кількість оборотних двійкових матриць такого розміру дорівнює $0,289\cdot2^{256}$, а кількість оборотних трійкових матриць ще значно вища: $0,56\cdot3^{256}$ [16].

Для забезпечення високого рівня стійкості довжина блока *r* і відповідний розмір матриць M_i повинні вибиратися так, щоб імовірність успішної атаки Єви *s* (2) після передачі *одного* блока була нехтовно малою величиною. Наприклад, для $s=10^{-4}$ величини *r* слід брати такими, як наведено в табл. 4. Матриці M_i передаються Бобові по звичайному відкритому (але автентифікованому) каналу 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 й, помноживши їх на відповідні блоки b_i, відновлює вихідні блоки повідомлення: $a_i=M_i^{-1}b_i$. Для квантового каналу зі значним рівнем шумів Аліса повинна спочатку передати деяку кількість блоків b_i достатню для того, щоб можна було зробити статистично значиму оцінку рівня помилок, які реєструються в режимі контролю підслуховування. Потім ця оцінка порівнюється з відомим заздалегідь граничним значенням природного рівня шумів у даному квантовому каналі. Якщо виконана оцінка рівня помилок перевищує допустиме значення, то сеанс зв'язку переривається, тому що це перевищення приписується підслуховуванню Єви, а підслуховування в пінг-понг протоколі створює досить високий додатковий рівень помилок (див. $d_{\max}$ у табл. 3). Інакше передається наступна послідовність блоків і знову виконується оцінка рівня помилок. Матриці M_i передаються всі разом тільки після успішного завершення квантового передавання. Описана процедура не є шифруванням повідомлення, а може бути названа оборотним гешуванням або гешуванням з використанням двосторонньої геш-функції, роль якої грає випадкова, оборотна над полем Галуа матриця чисел. Відзначимо, що у роботі [17] виконані оцінки обчислювальної складності генерації випадкових оборотних двійкових (розміру до 1000×1000) та трійкових (розміру до 200×200) матриць, та показано, що час генерації таких матриць прийнятний навіть при використанні обчислювальної техніки з невисокою швидкодією.

Завадостійке кодування для пінг-понг протоколу. При передаванні класичної інформації бітами єдиний можливий тип помилок – це переворот біта. У квантовому випадку будь-яке обертання або зміна фази в гільбертовому просторі квантового стану є помилкою, тобто існує нескінченна множина різних помилок, які можуть відбутися вже з одним, одиничним кубітом [18]. Для виправлення цієї неперервної множини помилок можна використовувати квантові завадостійкі коди, що виправляють деяку множину великих дискретних помилок: квантові завадостійкі коди, що виправляють деяку дискретну множину помилок, здатні автоматично виправляти безперервну множину помилок [1,18]. Така дискретизація квантових помилок в принципі дозволяє побудувати ефективні квантові завадостійкі коди. Але для квантових комунікаційних протоколів, зокрема протоколів квантового прямого безпечного зв’язку, немає необхідності використовувати квантові завадостійкі коди. Такі протоколи призначені для безпечного передавання *класичної* інформації. Тому для таких протоколів вигідніше використовувати *класичне завадостійке кодування*, яке має значно меншу надлишковість у порівнянні з квантовим завадостійким кодуванням. Крім того, класичне завадостійке кодування давно використовується в телекомунікаційних системах, розроблено методи побудови оптимальних кодів, існує

багатий практичний досвід їх використання. Теорія же квантових кодів, що виправляють помилки, знаходиться на теперішній час в стадії розробки [1,18].

Розглянемо детальніше, які помилки будуть виникати при реалізації пінг-понг протоколу в квантовому каналі з завадами. В протоколі з *n*-кубітними ГХЦ-станами для кодування рядка з *n* бітів використовується множина з 2^n ортогональних *n*-кубітних ГХЦ-станів. Боб виконує проективне вимірювання в *n*-кубітному ГХЦ-базисі й, при відсутності помилок, отримує один з цих станів з одиничною ймовірністю, а саме він отримує той стан, який відповідає кодувальній операції Аліси. Так, наприклад, нехай в протоколі з ГХЦ-триплетами Аліса бажає передати «011». Тоді, згідно з табл. 1, вона виконує операцію $i\sigma_y \otimes I$ над двома своїми кубітами, а Боб (при відсутності помилок) в результаті вимірювання над всіма трьома кубітами в ГХЦ-базисі з одиничною ймовірністю отримає стан $|\Psi_4\rangle = \left(|100\rangle - |011\rangle \right)/\sqrt{2}$. Якщо при передаванні кубітів в каналі відбудеться будь-яка помилка (не має значення, на прямому або зворотному шляху між Бобом та Алісою), то стан перед вимірюванням Боба буде вже не $|\Psi_4\rangle$, цей стан буде деякою суперпозицією всіх восьми три-кубітних ГХЦ-станів. Тоді результат проективного вимірювання Боба вже не буде давати «правильний» стан з одиничною ймовірністю, Боб може отримати будь-який з восьми станів з деякою ймовірністю, яка визначається амплітудою цього стану в суперпозиції. Отже Боб замість правильного рядка бітів з деякою ймовірністю отримує будь-який інший рядок. Підкреслимо, що немає необхідності виправляти сам ГХЦ-стан перед вимірюванням Боба, достатньо буде виправити бітовий рядок, який отримає Боб згідно з таблицею декодування (див. табл. 1). А ця задача може бути вирішена за допомогою класичних завадостійких кодів, що виправляють пакети помилок [19].

Вищенаведені міркування придатні для будь-якого варіанту пінг-понг протоколу. Помилки в бітових (або тритових для протоколу з кутритами) рядках будуть виникати пакетами, довжина яких буде дорівнювати інформаційної місткості протоколу на один раунд (див. табл. 3). Тому, ще одним структурним елементом квантової системи прямого безпечного зв'язку, що ґрунтується на пінг-понг протоколі, повинна бути система класичного завадостійкого кодування, яка містить в собі кодер на передавальній стороні та декодер на приймальній. Для завадостійкого кодування, в принципі, можна використовувати будь-який код, що виправляє пакети помилок заданої довжини, наприклад, код Файра або коди Ріда – Соломона [19]. Так, для протоколу з белівськими парами або ГХЦ-триплетами кубітів можна використовувати код Файра [42,33], який виправляє пакети помилок довжиною до трьох бітів і містить 33 інформаційних та 9 перевірочних бітів, тобто надлишковість цього коду дорівнює 27,3%. Обчислимо для порівняння надлишковість квантового коду Кальдербанка – Шора – Стіна (CSS-коду). Границя Варшамова-Гільберта для [*n*,*k*] CSS-коду, який виправляє помилки в *t* і менш кубітах [1]:

$$\frac{k}{n} \geq 1 - 2H\left(\frac{2t}{n}\right), \tag{4}$$

де $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ – двійкова ентропія.

При $k = 33$ і $t = 3$ з рівняння (4) одержуємо $n = 99$ кубітів, тобто довжина CSS-коду, який може виправити стани трьох кубітів в блоку з 33-х кубітів, повинна дорівнювати якнайменше 99 кубітам. Надлишковість коду в цьому випадку складає 200%, що майже у *8 разів* більше надлишковості класичного коду Файра, який виправляє пакети помилок довжиною до 3 бітів у 33-бітовому рядку. Відома також квантова границя Сінглтона, яка має місце для довільного квантового завадостійкого коду [1]: $n \geq 4t + k$. Підставляючи сюди $k = 33$ і $t = 3$, одержимо $n = 45$. Надлишковість буде 36,4%, що ненабагато більше надлишковості коду Файра. Але квантові завадостійкі коди, властивості яких наближаються до границі Сінглтона, на даний час невідомі. Таким чином, використання класичних завадостійких кодів для квантових протоколів прямого безпечного зв'язку, і зокрема пінг-понг протоколу, на даний час слід визнати кращим варіантом, ніж використання квантових кодів. Відзначимо, що для пінг-понг

протоколу замість кодів, що виправляють пакети помилок, можна також використовувати завадостійкі коди з перемежуванням [19]. Зрозуміло, що бажано було б знайти оптимальній завадостійкий код для кожного з варіантів пінг-понг протоколу. Ця задача виходить за рамки даної статті й буде предметом подальших досліджень.

Обговорення та висновки. В роботі розглядаються етапи синтезу структури квантових систем прямого безпечного зв'язку. За публікаціями автора та інших фахівців детально описані схеми етапів такого синтезу для систем, що ґрунтуються на різних варіантах пінг-понг протоколу. Так, першим етапом є розробка нового квантового протоколу (або вдосконалення за якимись параметрами вже існуючого), тобто розробка схеми квантового кодування інформації та схеми контролю перехоплення в квантовому каналі. Далі необхідно обчислити рівень стійкості протоколу до можливих видів атак, зокрема атаки пасивного перехоплення, тобто обчислити кількість інформації, яка може бути перехоплена зловмисником у залежності від параметрів протоколу. Наступний етап синтезу квантової системи безпечного зв'язку, який ґрунтується на отриманих результатах аналізу стійкості протоколу, – це розробка процедур підсилення стійкості. Так, процедура підсилення стійкості пінг-понг протоколу до атаки пасивного перехоплення дозволяє синтезувати систему безпечного зв'язку з наперед заданим рівнем стійкості до цієї атаки, оскільки розмір матриць для гешування вибирається з умови заданої, як завгодно малої, ймовірності невиявлення атаки. Також необхідно побудувати ефективний завадостійкій код, квантовий або класичний, з урахуванням особливостей передавання інформації в даному протоколі. На рис. 4 показана схема цих етапів.

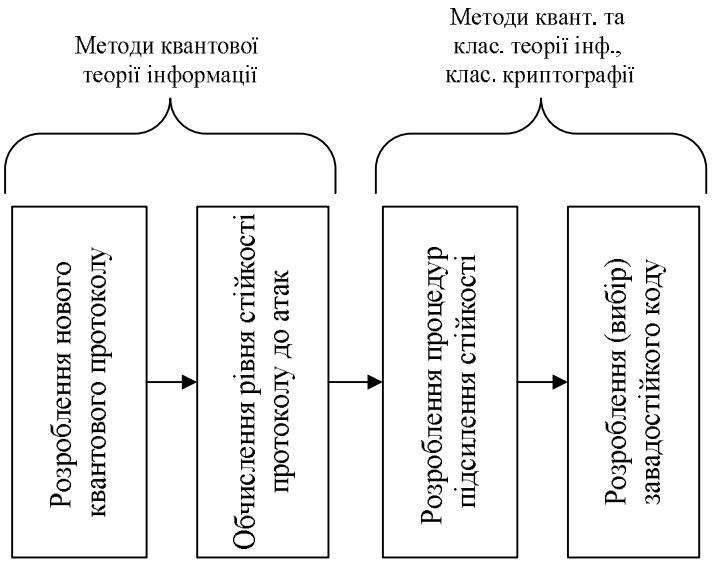

Рис. 4. Етапи структурного синтезу квантової системи прямого безпечного зв'язку

Відзначимо, що схема на рис. 4 придатна не тільки для систем, що ґрунтуються на пінг-понг протоколі, а і для систем, що ґрунтуються на протоколах квантового безпечного зв'язку з передаванням кубітів (кутритів і т.д.) блоками [7,10,15]. Ці протоколи мають безумовну, а не асимптотичну стійкість до атаки пасивного перехоплення, і тому не потребують описаної вище процедури підсилення стійкості. Але формула (2) для визначення кількості інформації, що утікає до Єви в пінг-понг протоколі, може бути використана для розрахунку мінімальної довжини блоку при перевірці підслуховування в протоколах з передаванням квантових систем блоками. В роботі описано використання класичних завадостійких кодів для реалізації квантових протоколів прямого безпечного зв'язку в квантовому каналі з завадами. Показано, що відомі на даний час класичні коди мають значно меншу надлишковість, ніж відомі квантові. Пошук оптимальних класичних кодів для різних варіантів пінг-понг протоколу буде предметом подальших досліджень.

ЛІТЕРАТУРА

1. Нильсен М. Квантовые вычисления и квантовая информация / Нильсен М., Чанг И. – М.: Мир, 2006. – 824 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. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, № 18. – 187902.

4. Ostermeyer M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, № 17. – P. 4540–4544.

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. 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.

7. 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, № 4. – 044305.

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. 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. – Vol. 341, № 5– 6. – P. 385–389.

10. 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, № 4. – 042317.

11. 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.

12. 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.

13. Ніколаєнко С.В. Виправлення помилок в пінг-понг протоколі квантового безпечного зв'язку / С.В. Ніколаєнко (наук. керівник Є.В. Василіу) // Теоретичні і прикладні проблеми фізики, математики та інформатики: збірка тез доповідей учасників VIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. – Київ: НТУУ «КПІ», 2010. – Ч. 2. – С. 92–93.

14. 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.

15. Wang Ch. Multi-step quantum secure direct communication using multi-particle Greenberger – Horne – Zeilinger state / Ch. Wang, F.-G. Deng, G.L. Long // Optics Communications. – 2005. – V. 253, № 1. – P. 15 – 20.

16. Overbey J. On the keyspace of the Hill cipher / J. Overbey, W. Traves, J. Wojdylo // Cryptologia. – 2005. – V. 29, № 1. – P. 59– 72.

17. Василіу Є.В. Оцінки обчислювальної складності способу підсилення безпеки пінг-понг протоколу з переплутаними станами кубітів та кутритів / Є.В. Василіу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 2. – С. 14–25.

18. Прескилл Дж. Квантовая информация и квантовые вычисления / Прескилл Дж. – Т. 1. – Ижевск: "Регулярная и хаотическая динамика", 2008. – 464 с.

19. Касами Т. Теория кодирования / Касами Т., Токура Н., Ивадари Ё. – М.: Мир, 1978. – 576 с.

Надійшла: 28.09.2012р.

Рецензент: д.т.н., проф. Дудикевич В.Б.