УДК 003.26:004.056.55:621.39

Корченко О.Г. (НАУ), Васіліу Є.В. (ОНАЗ), Гнатюк С.О. (НАУ), Кінзерявий В.М. (НАУ)

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РОБОТИ СИСТЕМИ КВАНТОВОГО ПРЯМОГО БЕЗПЕЧНОГО ЗВ'ЯЗКУ ІЗ ЗАСТОСУВАННЯМ ЗАВАДОСТІЙКИХ КОДІВ ДЛЯ КУТРИТІВ

У даній роботі розроблена математична модель системи квантового безпечного зв’язку на основі пінг-понг протоколу із застосуванням завадостійких кодів Ріда-Соломона над полем Галуа $GF(3^2)$. Формалізовано тритову систему завадостійкого кодування та детально описано роботу режиму передачі повідомлень пінг-понг протоколу з парами повністю переплутаних кутритів у каналі з шумом (деполяризуючому каналі). Крім того, на базі розробленого програмного забезпечення, проведено імітаційне (статистичне) моделювання роботи системи квантового прямого безпечного зв’язку, проаналізовано отримані результати та сформульовано практичні рекомендації.

Ключові слова: квантовий прямий безпечний зв'язок, пінг-понг протокол, деполяризуючий канал, завадостійкі коди, імітаційне моделювання, квантова кореляція.

Вступ. Сьогодні важко переоцінити важливість інформаційної безпеки в усіх галузях людської діяльності. Різке збільшення обсягів інформаційних ресурсів, як наслідок масової інформатизації, стало головним чинником проблеми забезпечення захищеності інформації від несанкціонованого доступу. Однією з головних характеристик захищеності інформації є конфіденційність, що забезпечується здебільшого криптографічними засобами захисту. Усі традиційні криптографічні методи базуються на гіпотетичній неможливості розв’язання певної математичної задачі за обмежений час. Принципово новим підходом є квантова криптографія, що ґрунтується на передачі інформації квантовими станами мікрочастинок. Надійність таких методів основана на принциповій непорушності законів квантової фізики. Більшість досліджень у даній галузі [1-3] присвячена протоколам квантового розподілу ключів, проте останнім часом значний інтерес викликає квантовий прямий безпечний зв'язок (КПБЗ). Основною відмінністю КПБЗ від інших квантових методів захисту інформації є відсутність будь-яких криптографічних перетворень (як наслідок відсутність актуальної в криптографії проблеми розподілу ключів шифрування). На теперішній час запропоновано кілька десятків різних за призначенням протоколів КПБЗ [1, 4, 5]. Серед них протоколи для безпосередньої передачі повідомлень між двома користувачами, протоколи для передачі повідомлень від одного користувача до іншого під контролем третьої довіреної сторони, протоколи для передачі повідомлень від одного користувача до багатьох (бродкастінг) і від багатьох до одного, а також протоколи квантових конференцій. Більшість із цих протоколів ґрунтується на створенні і подальшому розподілі між користувачами переплутаних (корельованих) [6, 7] станів двох або більшої кількості кубітів, що дозволяє передавати інформацію у двійковому вигляді. Інформаційну місткість протоколів КПБЗ можна збільшити за рахунок застосування квантового надщільного кодування [8] та використання багатовимірних квантових систем – кудитів (кутритів, куквартів і т.д.), а стійкість даних протоколів можна підвищувати за допомогою класичних математичних методів. З технологічної точки зору оперувати кудитами поки складніше, ніж кубітами, проте результати експериментів свідчать про перспективи реалізації практичних систем на їх основі уже в найближчому майбутньому.

Метою даної роботи є підвищення рівня доступності системи квантового прямого безпечного зв’язку за рахунок використання корегуючих кодів Ріда-Соломона над полем Галуа $GF(3^2)$. Для досягнення поставленої мети необхідно виконати такі **завдання:** 1) формалізувати тритову систему завадостійкого кодування; 2) дослідити роботу системи КПБЗ (на основі пінг-понг протоколу з парами повністю переплутаних кутритів) у режимі передачі повідомлень; 3) розробити алгоритми та програмне забезпечення, за допомогою якого провести імітаційне моделювання роботи даної системи; 4) проаналізувати отримані

статистичні дані та сформулювати практичні рекомендації щодо роботи пінг-понг протоколу у каналі з шумом.

1. Система завадостійкого кодування над полем Галуа GF(3^2).

Оскільки в реальних квантових каналах завжди є завади, то для практичної реалізації КПБЗ потрібні коди, що виправляють помилки. На даний час розроблені деякі сімейства квантових завадостійких кодів, що виправляють безпосередньо спотворені в каналі квантові стани [7]. Проте, практичне застосування таких кодів потребує використання квантових логічних гейтів [6, 7], що з технологічної точки зору поки що досить складно та нераціонально. Оскільки КПБЗ призначений для безпечного передавання *класичної* інформації квантовими каналами зв'язку, то можна кодувати класичними завадостійкими кодами безпосередньо класичну інформацію до її передавання квантовими частинками. У протоколах з групами *n* переплутаних кубітів інформація передається пакетами по *n* бітів, тому й помилки будуть виникати пачками відповідної довжини. Теорія двійкових кодів, що виправляють пачки помилок, на даний час розроблена достатньо повно, запропоновано велику кількість двійкових завадостійких кодів [9-12], що відрізняються надмірністю й корегувальною здатністю. Одними з таких є коди Ріда-Соломона (РС-коди), що використовуються для передачі в класичних каналах з високою інтенсивністю завад. Використання протоколів із парами переплутаних кутритів дозволяє збільшити інформаційну місткість, а як наслідок, швидкість передачі інформації, тому забезпечення її безпомилкової передачі такими протоколами є актуальною задачею, яку можна вирішити за допомогою трійкових РС-кодів. У роботі [13] детально описано трійкові РС-коди та виконано оцінку їх корегувальної здатності при передачі інформації з використанням переплутаних пар кутритів у квантовому каналі з шумом.

Для моделювання роботи системи КПБЗ необхідно формалізувати математичний апарат кодів відповідно до [9-12]. Нехай a – елемент поля GF(q^m) порядку *n*, де *q*, *m* – цілі числа, причому $q > 1$, $m > 0$ і $q^m \neq 2$. Якщо a - примітивний елемент, то його порядок дорівнює $(q^m - 1)$, тобто $a^{q^m-1} = 1$ і $a^i \neq 1$, де $0 < i < (q^m - 1)$. Тоді нормований поліном *g(x)* мінімального степеня над полем GF(q^m), розв'язками якого є $(d-1)$ степенів a^{i_0}, a^{i_0+1}, …, a^{i_0+d-2} елемента a, є породжувальним поліномом РС-кодів над полем GF(q^m): $g(x) = (x - a^{i_0})(x - a^{i_0+1})...(x - a^{i_0+d-2})$, де i_0 – деяке ціле число, за допомогою якого іноді вдається спростити процедуру кодування (зазвичай беруть $i_0 = 1$).

Довжина отриманого коду $n = q^m - 1$ символів і містить $r = d - 1 = \deg(g(x))$ перевірочних символів, де deg() означає степінь полінома, а d – мінімальна кодова відстань (мінімальна з усіх відстаней Хеммінга всіх пар кодових символів). Число інформаційних символів $k = n - r = n - d + 1$. Таким чином, $d = n - k + 1$. РС-коди виправляють $t = r/2$ помилок, але вимагають $r = 2t$ перевірочних символів. З їх допомогою виправляються довільні пачки помилок довжиною не більшою за t.

*Кодування***.** Для отримання закодованого поліному $C(x)$ необхідно до інформаційного поліному $S(x)$ додати $2t = r$ перевірочних символів так, щоб $C(x)$ ділився на $g(x)$ без лишку. Кодування може бути реалізовано двома способами: систематичним і несистематичним. При несистематичному кодуванні виконується саме перемноження $S(x)$ на $g(x)$: $C(x) = S(x) \cdot g(x)$, отриманий закодований поліном повністю відрізняється від початкового і для добування з нього $S(x)$ потрібно спочатку виконати повністю операцію декодування (незважаючи на відсутність помилок). Такий спосіб кодування вимагає великих витрат ресурсів лише на вилучення інформаційного поліному $S(x)$, при цьому він може бути без помилок. При систематичному кодуванні за відсутності помилок в $C(x)$ для отримання інформаційного полінома $S(x)$ потрібно лише відкинути $2t = r$ останніх символів.

Систематичне кодування відбувається у такий спосіб:

1) До $S(x)$ приписується $2t = r$ нулів, виходить поліном: $T(x) = S(x)x^{2t}$.

2) Поліном $T(x)$ ділиться на породжувальний поліном $g(x)$, знаходиться залишок $R(x)$: $T(x) = S(x)x^{2t} = Q(x)g(x) + R(x)$, де $Q(x)$ – частка.

3) Знаючи цей залишок визначається корегувальний РС-код, для цього від полінома $T(x)$ потрібно відняти $R(x)$. Отже, кодове повідомлення прийме вигляд: $C(x) = Q(x)g(x) = T(x) - R(x) = S(x)x^{2t} - R(x)$.

*Декодування***.** Нехай під час передачі на закодований поліном $C(x)$ подіяв шум $e(x)$: $Y(x) = C(x) + e(x)$. Для відновлення поліному $C(x)$ та інформаційного поліному $S(x)$ з отриманого $Y(x)$ потрібно виконати наступні операції:

1) Обчислення синдрому помилки. Для обчислення синдрому помилки $s(x)$, кодове слово $Y(x)$ ділять $g(x)$. Якщо залишок дорівнює нулю, кодове слово вважають не спотвореним, тобто $e(x) = 0$ та при систематичному кодуванні немає потреби проводити повну процедуру декодування, можна просто відкинути перевірочні символи і отримати інформаційний поліном $S(x)$. Ненульовий залишок свідчить про наявність принаймні однієї помилки. Залишок від ділення дає многочлен, що не залежить від $Y(x)$ і який визначений виключно характером помилки. Компоненти синдрому помилки можна також обчислювати за формулою $s_i = Y(a^i)$, де $i = 1,...,2t$, при чому $s_0 = 0$. Отримані компоненти об'єднують у синдром помилки у такий спосіб: $s(x) = \overline{s_{2t}s_{2t-1}...s_2s_1s_0}$. Якщо всі $s_i = 0$, при $i = 1,...,2t$, то $e(x) = 0$ і $Y(x) = C(x)$.

2) Обчислення локатора помилки. Отриманий синдром описує характер помилки, але не вказує на положення помилки. Для цього потрібно обчислити локатор помилки $L(x)$, коефіцієнти якого прямо відповідають коефіцієнтам спотворених символів. Якщо кількість спотворених символів не перевищує *t*, між $s(x)$ і $L(x)$ існує наступна однозначна відповідальність, що виражається наступною формулою $НОД(x^{n-1}, C(x)) = L(x)$, та обчислення локатора зводиться до задачі знаходження найменшого спільного дільника за алгоритмом Евкліда. На практиці зазвичай застосовують більш ефективний алгоритм Берлекемпа-Мессі.

3) Знаходження корнів локатора помилки. Найпростішим шляхом знаходження коренів многочлена $L(x)$ є метод проб і помилок, відомий як алгоритм Ченя. Цей алгоритм полягає в послідовному обчисленні $L(a^{-j})$ для кожного $j = 1,...,q-1$ та перевірки отриманих значень на нуль. Якщо величина $L(a^{-k})$ дорівнює нулю, то a^k є взаємним до кореня многочлена локаторів помилок і k -й елемент кодової комбінації містить помилку.

4) Визначення характеру помилки. Використовуючи синдром помилки і знайдені корні локатора помилок за допомогою алгоритму Форне визначається характер помилки і будується корегуючий поліном. Для цього потрібно виконати наступну послідовність операцій: а) обчислюється многочлен значень помилок $W(x)$: $W(x) = s(x) \cdot L(x) \bmod x^{2t}$; б) знаходиться похідна многочлена локатора помилок $L(x)$; в) знаходження корегувального полінома $e'(x)$: $e_l' = -\dfrac{W(X_l^{-1})}{L'(X_l^{-1})}$.

5) Виправлення помилки. Корегувальний поліном накладається на кодове слово і помилкові спотворені символи відновлюються: $C(x) = Y(x) + e'(x)$. Після цього з $C(x)$ відкидається перевірочні символи і відновлюється інформаційний поліном $S(x)$.

Оскільки, при передачі інформації квантовим каналом імовірність виникнення помилок досить велика, то було обрано РС-коди над полем Галуа GF(3^2), в яких $k = r$, що дозволяє виправляти $t = n/4$ пар помилкових тритів. При таких параметрах високий рівень надлишковості, проте виправляється велика кількість помилок. Також було обрано параметр $m = 2$, тоді $n = q^m - 1 = 3^2 - 1 = 9 - 1 = 8$ пар тритів, мінімальна кодова відстань $d = 5$, перевірочних символів $r = d - 1 = 5 - 1 = 4$ пари тритів, число інформаційних символів $k = n - r = 8 - 4 = 4$ пари тритів, кількість помилок які вдасться виправити $t = r/2 = 2$ пари тритів. Кодування і декодування виконувалось над примітивним поліном $x^2 + x + 2$ відповідно до роботи [13], у якій дані процеси представлені більш детально.

2. Особливості режиму передачі повідомлень пінг-понг протоколу з парами повністю переплутаних кутритів.

Розглянемо тепер детально режим передачі повідомлення пінг-понг протоколу з парами повністю переплутаних кутритів (рис. 1) [4]. Аліса (перший користувач – абонент відправник) заздалегідь розбиває свій рядок тритів на пари тритів. Якщо її повідомлення спочатку є бітовим (бінарним) рядком, то його необхідно перетворити в рядок тритів. Далі виконуються такі кроки:

1) Боб (другий користувач – абонент отримувач) готує пару кутритів у початковому стані $|\Psi_{00}\rangle = \left(|00\rangle + |11\rangle + |22\rangle\right)/\sqrt{3}$. У цьому випадку кутрит є одиночним фотоном, а пара таких кутритів – фотонів переплутується по їх орбітальному кутовому моменту.

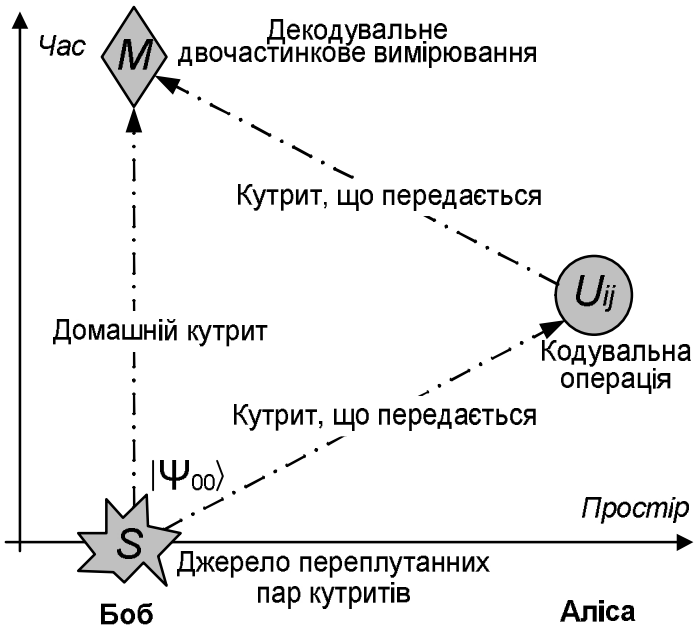


Рис.1. Режим передачі повідомлення пінг-понг протоколу КПБЗ

2) Боб залишає у себе перший кутрит ("домашній") і відправляє Алісі другий ("що передається") квантовим каналом зв'язку (у якості якого може використовуватись одномодова оптоволоконна лінія або відкритий простір – оптичний бездротовий канал).

3) Аліса отримує кутрит, що передається, від Боба. З імовірністю *q* вона переходить в режим контролю підслуховування і виконується крок 4, у іншому випадку Аліса переходить у режим передачі повідомлення і виконуються кроки з 5-го по 7-ий.

4) Контроль підслуховування виконується так званими одночастинковими квантовими вимірюваннями станів кутритів одночасно Алісою й Бобом у різних базисах, що детально описано у роботі [14].

5) У відповідності зі своїм поточним двотритовим рядком, Аліса вибирає одну з дев'яти (у випадку з кутритами) кодувальних операцій і виконує дану операцію (за допомогою

квантових логічних гейтів) над отриманим від Боба кутритом. При цьому, початковий стан пари кутритів $|\Psi_{00}\rangle$ перетвориться відповідно до операції, виконаної Алісою [4]. Потім Аліса відправляє кутрит назад Бобу квантовим каналом (див. рис. 1).

6) Отримавши кутрит, що передається, від Аліси, Боб виконує декодувальне двочастинкове вимірювання над парою кутритів в базисі Бела для кутритів, що дозволяє йому достовірно визначити стан, створений кодувальною операцією Аліси, і тим самим визначити двотритовий рядок, який вона послала.

7) Якщо повідомлення передано повністю, то протокол успішно закінчений, інакше відбувається перехід до кроку 1.

3. Імітаційне моделювання роботи системи КПБЗ у режимі передачі повідомлень.

Будь-яка система зв'язку схильна дії шумів, які приводять до неправильного прийому сигналу. Високоефективним засобом вирішення даної проблеми є застосування завадостійкого кодування, заснованого на введенні штучної надлишковості в повідомленнях, що передаються. На рис. 2 зображено математичну модель роботи системи КПБЗ у режимі передачі повідомлень із застосуванням РС-кодів для кутритів.

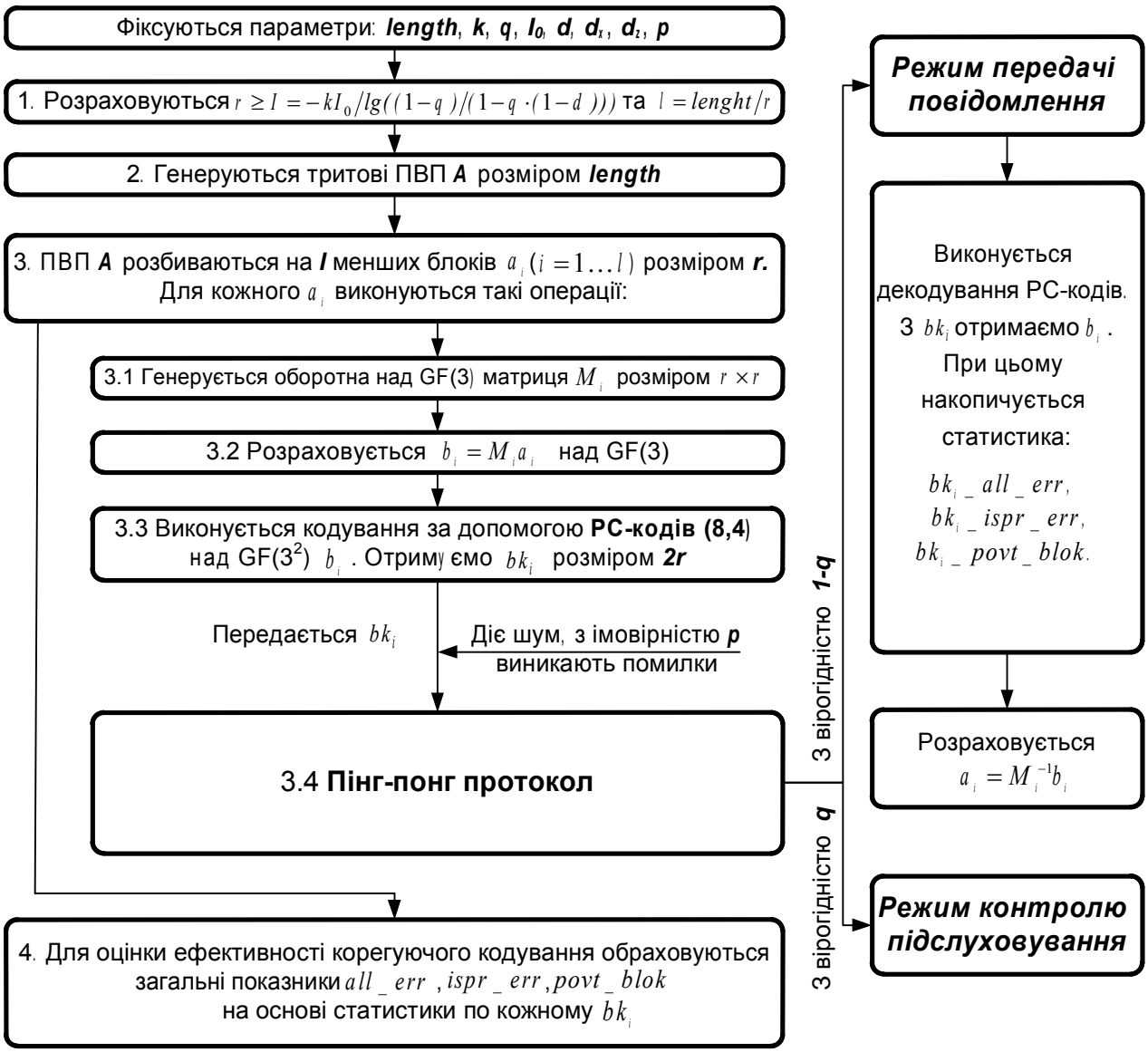


Рис.2. Математична модель роботи системи КПБЗ у режимі передачі повідомлень із застосуванням РС-кодів для купритів

Оригінальний пінг-понг протокол має лиш асимптотичну стійкість, тому для підсилення рівня безпеки нашої системи пропонується застосувати метод підсилення, запропонований у [15]. Даний метод полягає у наступному: Аліса розбиває своє трійкове повідомлення на l блоків $a_i\ (i = 1 \ldots l)$ довжини r, після чого для кожного блоку окремо генерує випадкову, оборотну над GF(3) трійкову матрицю M_i розміром $r \times r$ та перемножує їх $b_i = M_i a_i$. Отримані в результаті блоки передаються квантовим каналом за пінг-понг протоколом. Навіть якщо Єва (несанкціонований користувач, зловмисник) перехопить один (або декілька) із цих блоків, залишившись невиявленою, то, не знаючи використаних матриць M_i, вона не зможе відновити блоки a_i. Матриці M_i передаються Бобу відкритим каналом після завершення квантового передавання, але тільки в тому випадку, якщо Аліса й Боб переконалися у відсутності підслуховування в квантовому каналі. Саме цей факт і відрізняє даний метод від шифру Хіла, де матриці є ключами, а використання одноразових матриць забезпечує стійкість методу до уразливостей, характерних згаданому шифру [16]. Потім Боб відновлює блоки даних відповідно до виразу $a_i = M_i^{-1} b_i$. Довжина блока $r \geq l = -kI_0 / lg((1-q)/(1-q \cdot (1-d)))$ і відповідний розмір матриць $M_i\ (r \times r)$ обирається так, щоб імовірність успішної атаки Єви s, після передачі одного блока, була нехтовно малою величиною $s(l, q, d) = 10^{-k}$, де I – кількість інформації, що отримує Єва при передаванні одного блока, I_0 – кількість інформації, що отримує Єва за один раунд протоколу, q – імовірність переходу в режим контролю підслуховування, d – рівень помилок, що створює Єва, k – показник степені десятки для обрахунку ймовірності невиявлення атаки Єви (фіксований коефіцієнт рівня безпеки системи). На рис. 3 зображено критерій стійкості даного методу, тобто залежність кількості необхідних операцій, що треба виконати для підбору матриць, від безпосередньої величини даних трійкових матриць.

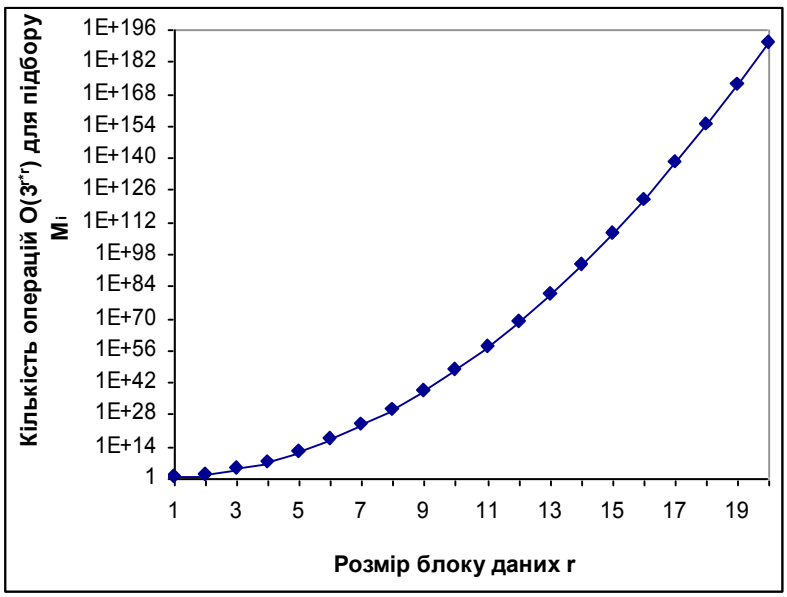


Рис.3. Критерій стійкості методу підсилення до лобової атаки

Для моделювання роботи системи КПБЗ на основі пінг-понг протоколу з парами кутритів і застосуванням РС-кодів були використані такі вхідні параметри: 1) *length* = 100 000 трит – довжина передаваних трійкових даних; 2) k = 4 (зафіксували необхідний рівень безпеки); 3) q = 0.5 – імовірність перемикання протоколу в режим контролю підслуховування та $(1-q)$ – імовірності перемикання в режим передавання повідомлення (дана стратегія перемикання між режимами вважається [4] найоптимальнішою для Аліси і

Боба); 4) Для розрахунку величини *r* бралось: $l_0 = 2$ – кількість інформації, яку могла отримати Єва за один раунд (припускали, що Єва могла отримати повну інформацію за один раунд, тобто 2 трити), $d = 1/3$ – рівень помилок, що створювала б Єва (припускали, що Єва створювала б мінімально можливий рівень помилок, див. [13]); 5) p = 0;…;0,5 – рівень (ймовірність) деполяризації (перебирали з кроком 0,01).

Параметр ***p*** фіксувався, після чого виконувались такі операції:

Перший крок. З огляду на необхідний рівень безпеки, розраховувалась довжина блоку даних *r* [14] та кількість самих блоків *l*, на які розбивались передавані дані. Для зручності застосування РС-кодів *r* вибиралось кратним 8, а ввеличина *l* вираховувалась за формулою $l = lenght\ /r$.

Другий крок. Генерувались трійкові псевдовипадкові послідовності (ПВП) розміром *length* (імовірність генерації "0", "1", "2" бралась рівною $1/3$).

Третій крок. Згенеровані в п. 2 ПВП 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 такі операції:

1. Для кожного блоку a_i генерувалась випадкова, оборотна над полем GF(3) матриця M_i розміром $r \times r$.

2. Виконувалось перемноження $M_i a_i$ в полі Галуа GF(3), в результаті отримували b_i .

3. Далі отримане b_i розбивали на підблоки по 8 тритів і за допомогою РС-кодів проводили їх кодування, у результаті кожен підблок збільшував свою довжину до 16 тритів, після чого під блоки назад об'єднували і отримували блок bk_i розміром *2r*.

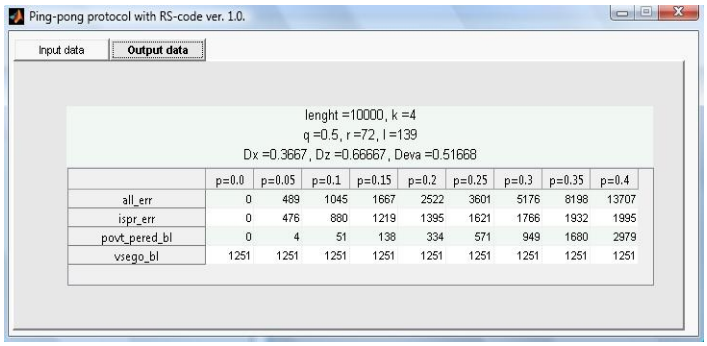
4. Далі виконувалась передача bk_i за допомогою пінг-понг протоколу квантовим каналом з шумом. З ймовірностями q та $(1-q)$ відбувалось перемикання в режим контролю підслуховування та в режим передавання повідомлення відповідно. Перемикання між режимами відбувалось доти, поки не передавався повністю блок bk_i .

У ***режимі контролю підслуховування*** моделювання не виконувалось, моделювання цього режиму виконано у роботі [14]. У ***режимі передачі повідомлення*** моделювалось приймання Бобом по черзі кожної пари тритів блоку bk_i через квантовий канал (помилки, тут обумовлені тільки шумом в каналі, оскільки ми припускали (вважали), що Єва не виконує підслуховування). Кожні 8 пар прийнятих тритів блоку bk_i намагались декодувати за допомогою РС-кодів. Якщо кількість спотворених шумом пар тритів була менше трьох, коди їх безпомилково виправляли, в іншому випадку ці 8 пар тритів передавали повторно (тобто використовується так зване корегуюче кодування зі зворотнім зв'язком). У результаті декодування РС-кодами з bk_i отримували b_i розміром *r*. При моделюванні помилок у каналі з шумом ***врахували симетрію деполяризуючого каналу (ДПК)***, а саме імовірність $p/8$ заміни відповідної пари тритів на одну з 8-ми інших. Наступним кроком було відновлення вихідного повідомлення a_i, для цього виконувалось перемноження $M_i^{-1} b_i$ в полі Галуа GF(3). Для кожного переданого блоку bk_i обраховувались $bk_i\_all\_err$, $bk_i\_ispr\_err$, та $bk_i\_povt\_blok$, (кількість помилок, кількість виправлених помилок та кількість разів повторного передавання даного підблоку відповідно).

Четвертий крок. На основі зібраної статисти по кожному bk_i, обраховувались загальні показники all_err, $ispr\_err$ та $povt\_blok$, які необхідні були для оцінки рівня доступності системи КПБЗ у ДПК із використанням запропонованих РС-кодів.

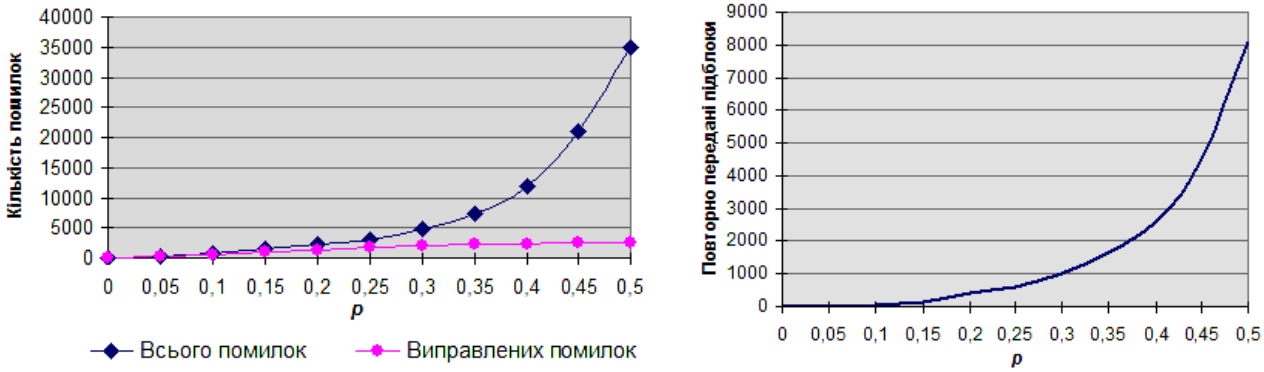
4. Аналіз результатів моделювання та формулювання практичних рекомендацій.

З метою проведення статистичного моделювання роботи системи КПБЗ у режимі передачі повідомлень (із застосуванням РС-кодів для кутритів та методу підсилення секретності) у середовищі MATLAB R2009b було розроблено відповідне програмне забезпечення (рис. 4). У результаті моделювання отримано статистичні дані, на основі яких побудовані графіки (рис. 5), які підтверджують придатність даних кодів для корекції помилок при реалізації типових протоколів КПБЗ у ДПК. Зокрема, отримана статистична інформація показує, що коди добре справляються з корекцією помилок, якщо ймовірність деполяризації кутритів p у квантовому каналі не перевищує 25-30%. При $p = 25\%$ кількість повторно переданих підблоків складає 46,7%, а при $p = 30\%$ – 81,4% від їх загальної кількості. При $p = 10\%$ кількість повторно переданих підблоків складає всього 3,8% від їх загальної кількості. Оскільки в сучасних експериментах рівень помилок при передаванні фотонів квантовим каналом, як правило, не перевищує декількох відсотків, то можна зробити висновок, що трійкові РС-коди цілком придатні для корегуючого кодування в типових протоколах КПБЗ з передаванням кутритів.



	p=0.0	p=0.05	p=0.1	p=0.15	p=0.2	p=0.25	p=0.3	p=0.35	p=0.4
all_err	0	489	1045	1667	2522	3601	5176	8198	13707
ispr_err	0	476	880	1219	1395	1621	1766	1932	1995
povt_pered_bl	0	4	51	138	334	571	949	1680	2979
vsego_bl	1251	1251	1251	1251	1251	1251	1251	1251	1251

Рис.4. Інтерфейс програмного засобу для моделювання роботи пінг-понг протоколу у режимі передачі повідомлень



а *б*

Рис.5. Залежність від деполяризації p: а) кількості отриманих та виправлених помилок; б) кількості повторно переданих підблоків

Проте, вказане відсоткове обмеження не є критичним і може змінюватися експертним методом в залежності від умов експлуатації, очікуваного рівня безпеки, часових обмежень та інших чинників. Таким чином, отримані результати можуть слугувати вагомим інструментальним засобом експерта у сфері інформаційної безпеки при побудові ефективних систем КПБЗ.

Висновки. Таким чином, у даній статті виконані дослідження, що у сукупності дозволяють підвищити рівень доступності системи КПБЗ. У роботі формалізовано тритову систему завадостійкого кодування, досліджено роботу системи КПБЗ на основі удосконаленого пінг-понг протоколу з парами повністю переплутаних кутритів у режимі передачі повідомлень. На основі даних досліджень розроблено математичну модель системи КПБЗ із застосуванням завадостійких РС-кодів над скінченним полем Галуа $GF(3^2)$ у режимі передачі повідомлень. Крім того, розроблено програмне забезпечення, за допомогою якого проведено імітаційне моделювання роботи даної системи КПБЗ. У результаті моделювання отримано статистичні дані, які підтверджують придатність даних кодів для корекції помилок

та здатність забезпечувати високу доступність квантового каналу при реалізації типових протоколів. Крім того, отримані результати можуть слугувати ефективним інструментарієм експерта у сфері інформаційної безпеки при побудові ефективних квантових СЗІ.

Література:

1. Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius : Technika, 2010, Vol. 14, № 2, p. 58–69.

2. Румянцев К.Е. Квантовая связь и криптография: Учебное пособие / К.Е. Румянцев, Д.М. Голубчиков — Таганрог: Изд-во ТТИ ЮФУ, 2009. — 122 с.

3. Килин С.Я. Квантовая криптография : Идеи и практика : Монография / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. — Мінськ, 2008. — 398 с.

4. 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.

5. Bostrom K. Deterministic secure direct communication using entanglement / Bostrom K., Felbinger T. // Physical Review Letters. — 2002. — V. 89, № 18. — Art. 187902.

6. Физика квантовой информации : Квантовая криптография. Квантовая телепортация. Квантовые вычисления / Ред. Д. Боумейстер [и др.] ; Пер. с англ. С.П. Кулик, Е.А. Шапиро ; Ред. пер. С.П. Кулик, Т.А. Шмаонов. — М. : Постмаркет, 2002. — С. 33–73.

7. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. — М. : Мир, 2006. — 824 с.

8. 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.

9. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут; пер. англ. И.И. Грушко, В.М. Блиновского. — М. : Мир, 1986. — 576 с.

10. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. — М. : Техносфера, 2005. — 320 с.

11. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж.А. Слоэн. — М. : Связь, 1979. — 744 с.

12. Вернер М. Основы кодирования: учебник для ВУЗов / М. Вернер. — М. : Техносфера, 2004. — 288 с.

13. Оцінка корегувальної здатності завадостійких трійкових РС-кодів при передачі інформації повністю переплутаними станами кутритів квантовим каналом із шумом / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Захист інформації. — 2010. — № 4. — С. 44–53.

14. Імітаційна модель пінг-понг протоколу з парами переплутаних кутритів у квантовому каналі з шумом / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Захист інформації. — 2010. — № 3. — С. 46–56.

15. 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.

16. Математичні основи криптоаналізу: Навч. посібник / С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. — Д. :Національний гірничий університет, 2010. — 465 с.

Надійшла: 25.05.2011 р.

Рецензент: д.т.н., проф. Конахович Г.Ф.