УДК 003.26:004.056.55:621.39

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

ОЦІНКА КОРЕГУВАЛЬНОЇ ЗДАТНОСТІ ЗАВАДОСТІЙКИХ ТРІЙКОВИХ РС-КОДІВ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ ПОВНІСТЮ ПЕРЕПЛУТАНИМИ СТАНАМИ КУТРИТІВ У КВАНТОВОМУ КАНАЛІ З ШУМОМ

Вступ. У сучасному інформаційному суспільстві все більша кількість людей відчуває потребу в конфіденційному зв'язку. Квантові комунікації, які ґрунтуються на передачі інформації, закодованої у квантових станах мікрочастинок, пропонують ряд нових способів для безпечного обміну повідомленнями [1]. Одним з напрямів квантових комунікацій є квантовий прямий безпечний зв'язок (КПБЗ), де легітимні користувачі обмінюються квантовими частками квантовим каналом зв'язку, виконують певні операції і вимірювання над цими частками, а також обмінюються додатковою інформацією звичайним (не квантовим) каналом з автентифікацією [2-14]. Практично, в якості квантових часток використовують фотони, так як вони є найбільш стабільними носіями квантової інформації, а у якості квантових каналів – оптоволоконні лінії зв'язку або атмосферу (оптичний бездротовий канал). При цьому, безпека передачі інформації з використанням протоколів КПБЗ гарантується законами квантової фізики.

На теперішній час запропоновано декілька десятків різних за призначенням протоколів КПБЗ. Серед них протоколи для безпосередньої передачі повідомлень між двома користувачами [2-5], протоколи для передачі повідомлень від одного користувача до іншого під контролем третьої довіреної сторони [6,7], протоколи для передачі повідомлень від одного користувача до багатьох (бродкастінг) і від багатьох до одного, а також протоколи квантових конференцій [8-11]. Більшість із цих протоколів ґрунтується на створенні і подальшому розподілі між користувачами переплутаних станів двох або більшої кількості кубітів, що дозволяє передавати інформацію у двійковому вигляді.

У роботі [2] представлено один з простих протоколів КПБЗ із використанням пар повністю переплутаних кубітів, який має інформаційну місткість в 1 біт на цикл протоколу. Використовуючи квантове надщільне кодування для кубітів, можна збільшити інформаційну місткість до 2 бітів на цикл [12,13]. Далі, для реалізації протоколу можна використовувати переплутані трійки, четвірки і т.д. кубітів [14]. Протокол з групами n переплутаних кубітів, що перебувають в станах Грінбергера – Хорна – Цайлінгера, та квантовим надщільним кодуванням має інформаційну місткість n бітів на цикл [15]. На даний час в експериментах досягнуто переплутування групи з 10 кубітів, проте поки що це технологічно достатньо складна операція [16].

З іншого боку, інформаційну місткість протоколів КПБЗ можна збільшити, використовуючи замість кубітів багатовимірні квантові системи (кудити) та так зване квантове надщільне кодування для кудитів. Так, протокол з переплутаними парами тривимірних квантових систем (кутритів) буде мати місткість $\log_2 9 \approx 3{,}17$ бітів на цикл замість двох бітів на цикл для протоколу з парами кубітів [17,18]. З технологічної точки зору оперувати кутритами поки складніше, ніж кубітами, проте ряд експериментів щодо створення переплутаних пар кутритів вже виконано [19,20].

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 зіпсовані в каналі квантові стани [1]. Проте практичне застосування таких кодів потребує використання квантових логічних елементів (елементів квантового комп'ютера), 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 [21-27], що відрізняються надмірністю й виправлювальною (корегувальною) здатністю. Одними з таких є коди Ріда-Соломона (РС), що використовуються для передачі в класичних каналах з високою інтенсивністю завад, коли виникають помилки кратністю дві й більше, пачки помилок, а також сполучення пачок і однократних помилок [21-26].

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. Проте в літературі [21-26] трійкові коди практично не висвітлені, тому є необхідність їх детального розгляду з метою випробування їх корегувальної здатності при передачі інформації квантовим каналом із шумом. Таким чином, **метою** даної роботи є оцінка корегувальної здатності трійкових РС-кодів при передачі інформації з використанням переплутаних пар кутритів у квантовому каналі з шумом.

1. Коди Ріда-Соломона над полем Галуа GF(3^2). РС-коди є важливим окремим випадком коду БЧХ, розв'язки породжувального полінома якого лежать в тому ж полі, над яким і будується код. Для наочності опишемо РС-коди в їх загальному вигляді відповідно до [21-26]. 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):

$$g(x)=(x-a^{i_0})(x-a^{i_0+1})...(x-a^{i_0+d-2}), \qquad (1)$$

де i_0 – деяке ціле число, за допомогою якого іноді вдається спростити процедуру кодування. Зазвичай беруть $i_0=1$. Степінь многочлена $g(x)$ дорівнює $(d-1)$.

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, $d=n-k+1$, коди з подібним значенням мінімальної кодової відстані в теорії кодування отримали назву максимальних. 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. Згідно теоремі про границю Рейгера, РС-коди є оптимальними з точки зору співвідношення довжини пакету та можливості виправлення помилок.

*Кодування***.** Для отримання закодованого поліному $C(x)$ необхідно в інформаційний поліном $S(x)$ добавити $2t=r$ 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 операцію декодування (незважаючи на наявність помилок). Такий спосіб кодування вимагає великих витрат ресурсів лише на вилучення інформаційного поліному $S(x)$, при цьому він може бути без помилок. При симетричному кодуванні при відсутності помилок в $C(x)$ для отримання інформаційного полінома $S(x)$, потрібно лише відкинути $2t=r$ останніх символів.

Симетричне 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 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 звичайно 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 корегувальний 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, в даній роботі досліджується корегувальна здатність РС-кодів над полем Галуа GF(3^2), в яких $k = r$, що дозволяє виправляти $t = n/4$ пар помилкових тритів. Отже, у роботі використовуються наступні параметри: довжина отриманого коду $n = q^m - 1 = 3^2 - 1 = 9 - 1 = 8$ 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.

Для знаходження породжувального многочлена спочатку необхідно описати операції додавання та множення в полі Галуа GF(3^2). Поле Галуа GF(3^2) може бути побудоване над такими поліномами x^2+1, x^2+x+2, x^2+2x+2, $2x^2+2$, $2x^2+x+1$, $2x^2+2x+1$. У даній

роботі для побудови поля Галуа GF(3^2) використовувався примітивний поліном x^2+x+2. Позначимо всі можливі пари тритів, як показано в табл. 1 у поліноміальному вигляді. Тоді, якщо позначити x як примітивний елемент a, можна з легкістю порахувати будь-яку трійкову пару у вигляді степеня a. Для цього необхідно перемножити відомі поліноміальні позначення степенів a по модулю x^2+x+2, результат показаний в табл.1.

Таблиця 1. Елементи поля Галуа GF(3^2) над поліномом x^2+x+2

В трійковому вигляді	У вигляді полінома	У вигляді степені
00	0	0
01	1	$a^8=1$
02	2	$a^4=2$
10	x	a^1
11	x+1	a^7
12	x+2	a^6
20	2x	a^5
21	2x+1	a^2
22	2x+2	a^3

На основі табл.1. були побудовані необхідні таблиці додавання та множення в полі Галуа GF(3^2) над примітивним поліномом x^2+x+2 (див. табл. 2 та табл. 3), результати операцій віднімання і ділення можна з легкістю отримати з тих же таблиць.

Таблиця 2. Додавання в полі Галуа GF(3^2) над поліномом x^2+x+2

+	**0**	$\boldsymbol{a^8=1}$	$\boldsymbol{a^4=2}$	$\boldsymbol{a^1}$	$\boldsymbol{a^7}$	$\boldsymbol{a^6}$	$\boldsymbol{a^5}$	$\boldsymbol{a^2}$	$\boldsymbol{a^3}$
0	0	$a^8=1$	$a^4=2$	a^1	a^7	a^6	a^5	a^2	a^3
$\boldsymbol{a^8=1}$	$a^8=1$	$a^4=2$	0	a^7	a^6	a^1	a^2	a^3	a^5
$\boldsymbol{a^4=2}$	$a^4=2$	0	$a^8=1$	a^6	a^1	a^7	a^3	a^5	a^2
$\boldsymbol{a^1}$	a^1	a^7	a^6	a^5	a^2	a^3	0	$a^8=1$	$a^4=2$
$\boldsymbol{a^7}$	a^7	a^6	a^1	a^2	a^3	a^5	$a^8=1$	$a^4=2$	0
$\boldsymbol{a^6}$	a^6	a^1	a^7	a^3	a^5	a^2	$a^4=2$	0	$a^8=1$
$\boldsymbol{a^5}$	a^5	a^2	a^3	0	$a^8=1$	$a^4=2$	a^1	a^7	a^6
$\boldsymbol{a^2}$	a^2	a^3	a^5	$a^8=1$	$a^4=2$	0	a^7	a^6	a^1
$\boldsymbol{a^3}$	a^3	a^5	a^2	$a^4=2$	0	$a^8=1$	a^6	a^1	a^7

Для розрахунку породжувального полінома брали $i_0=1$, використовували формулу (1) і таблиці 1, 2, 3:

$$g(x)=(x-a^1)(x-a^2)(x-a^3)(x-a^4)=x^4+a^7x^3+a^2x^2+a^4x+a^2=\overline{a^8a^7a^2a^4a^2}.$$

Знаючи $g(x)$, n, k, r – РС-коди можуть застосовуватись на практиці.

Таблиця 3. Множення в полі Галуа GF(3^2) над поліномом $x^2 + x + 2$

x	**0**	a^8**=1**	a^4**=2**	a^1	a^7	a^6	a^5	a^2	a^3
0	0	0	0	0	0	0	0	0	0
a^8**=1**	0	a^8=1	a^4=2	a^1	a^7	a^6	a^5	a^2	a^3
a^4**=2**	0	a^4=2	a^8=1	a^5	a^3	a^2	a^1	a^6	a^7
a^1	0	a^1	a^5	a^2	a^8=1	a^7	a^6	a^3	a^4=2
a^7	0	a^7	a^3	a^8=1	a^6	a^5	a^4=2	a^1	a^2
a^6	0	a^6	a^2	a^7	a^5	a^4=2	a^3	a^8=1	a^1
a^5	0	a^5	a^1	a^6	a^4=2	a^3	a^2	a^7	a^8=1
a^2	0	a^2	a^6	a^3	a^1	a^8=1	a^7	a^4=2	a^5
a^3	0	a^3	a^7	a^4=2	a^2	a^1	a^8=1	a^5	a^6

Приклад 1. Для наочності кодування РС кодів (8,4) над полем Галуа GF(3^2) наведемо невеликий приклад. Нехай інформаційний поліном $S(x)$ містить 4 пари тритів: 22 21 01 11, потрібно його закодувати, для цього виконаємо наступну послідовність операцій:

1) Переведемо $S(x)$ з трійкового в степеневий вигляд за табл. 1:

$S(x) = \overline{22210111} = \overline{a^3 a^2 a^8 a^7}$.

2) До $S(x)$ припишемо $2t = r = 4$ нулів:

$T(x) = S(x)x^4 = \overline{a^3 a^2 a^8 a^7 0000}$.

3) За допомогою табл. 2, 3 виконаємо ділення $T(x)$ на розрахований вище $g(x)$.

Знайдемо залишок $R(x)$ як показано на рис.1.

$$
\begin{array}{l|l}
a^3x^7+a^2x^6+a^8x^5+a^7x^4 & a^8x^4+a^7x^3+a^2x^2+a^4x+a^2 \\
\underline{a^3x^7+a^2x^6+a^5x^5+a^7x^4+a^5x^2} & a^3x^3+a^7x+a^2 \quad - \ Q(x) \\
\quad a^7x^5+a^1x^3 & \\
\quad \underline{a^7x^5+a^6x^4+a^1x^3+a^3x^2+a^1x} & \\
\qquad a^2x^4+a^7x^2+a^5x & \\
\qquad \underline{a^2x^4+a^1x^3+a^4x^2+a^6x+a^4} & \\
R(x) - \quad a^5x^3+a^6x^2+a^7x+a^8 &
\end{array}
$$

Рис. 1. Знаходження залишку $R(x)$ при діленні $T(x)$ на $g(x)$

Отже, $R(x) = \overline{a^5 a^6 a^7 a^8}$.

4) За допомогою табл. 2 розрахуємо $C(x)$:

$C(x) = Q(x)g(x) = T(x) - R(x) = \overline{a^3 a^2 a^8 a^7 0000} - \overline{a^5 a^6 a^7 a^8} = \overline{a^3 a^2 a^8 a^7 a^1 a^2 a^3 a^4}$.

Переведемо отриманий $C(x)$ у трійковий вид за табл. 1, який і буде закодованою послідовністю: $C(x) = \overline{a^3 a^2 a^8 a^7 a^1 a^2 a^3 a^4} = \overline{2221011110212202}$.

Приклад 2. Для наочності декодування РС кодів (8,4) над полем Галуа GF(3^2) наведемо невеликий приклад. Нехай на закодований поліном, показаний в прикладі 1, $C(x) = \overline{2221011110212202}$ (у степеневому вигляді $C(x) = \overline{a^3 a^2 a^8 a^7 a^1 a^2 a^3 a^4}$) подіяв шум $e(x) = \overline{0021000000110000}$ (у степеневому вигляді $e(x) = \overline{0a^2 000a^7 00}$), у результаті був отриманий многочлен $Y(x)$:

$Y(x) = C(x) + e(x) = \overline{2221011110212202} + \overline{0021000000110000} = \overline{2212011110022202}$.

У степеневому вигляді та поліноміальному вигляді $Y(x) = \overline{a^3 a^6 a^8 a^7 a^1 a^4 a^3 a^4} =$

$= a^3x^7 + a^6x^6 + a^8x^5 + a^7x^4 + a^1x^3 + a^4x^2 + a^3x + a^4$, потрібно за допомогою РС-кодів (8,4) декодувати та виправити $Y(x)$. Для цього виконаємо наступну послідовність операцій:

1) Обчислимо компоненти синдрому помилки $S(x)$, використовуючи співвідношення $a^8 = 1$ та табл. 2, 3:

$s_1 = Y(a^1) = a^{10} + a^{12} + a^{13} + a^{11} + a^4 + a^6 + a^4 + a^4 = a^2 + a^4 + a^5 + a^3 + a^4 + a^6 + a^4 + a^4 =$

$= a^5 + a^6 + a^7 + a^8 = a^4 + a^6 = a^7$

$s_2 = Y(a^2) = a^{17} + a^{18} + a^{18} + a^{15} + a^7 + a^8 + a^5 + a^4 = a^1 + a^2 + a^2 + a^7 + a^7 + a^8 + a^5 + a^4 =$

$= a^8 + a^4 + a^6 + a^3 = 0 + a^8 = a^8$

Аналогічно обраховувалися інші компоненти синдрому помилки.

$s_3 = Y(a^3) = a^3$

$s_4 = Y(a^4) = a^4$

Отже, синдром помилки $S(x) = \overline{a^4 a^3 a^8 a^7 0} = a^4 x^4 + a^3 x^3 + a^8 x^2 + a^7 x$.

2) Обчислюємо локатор помилки алгоритмом Берлекемпа-Мессі, використовуючи табл. 1, 2, 3.

Для цього, введемо деякі змінні та їх початкові значення: $r = 0$ – номер ітерації, $L = 0$, $B(x) = 1$- нормуюча добавка, $L(x) = 1$ – початковий локатор помилки. Їх будемо змінювати під час виконання кожної з $2t$ ітерацій, поки не отримаємо кінцевий варіант локатора помилки $L(x)$.

Опишемо виконання кожної ітерації:

1. Для $r = 1$ спочатку знайдемо Δr – помилку в наступному компоненті синдрому:

$$\Delta r = \sum_{j=0}^{L} L_j s_{r-j} = \sum_{j=0}^{0} L_j s_{1-j} = L_0 s_1 = 1 \cdot a^7 = a^7 .$$

Оскільки $\Delta r \neq 0$ обчислимо новий многочлен зв'язків:

$M(x) = L(x) - \Delta r \cdot x \cdot B(x) = 1 - a^7 \cdot x \cdot 1 = a^3 x + 1$.

Оскільки виконується нерівність $2L = 0 \le (r-1) = 0$ обчислимо нову нормуючу добавку $B(x)$, новий локатор помилки $L(x)$ і L:

$B(x) = \Delta r^{-1} \cdot L(x) = a^{-7} \cdot 1 = a^1$, $L(x) = M(x) = a^3 x + 1 = \overline{a^3 a^8}$, $L = r - L = 1 - 0 = 1$.

Оскільки $r \neq 2t$, переходимо до наступної ітерації $r = r + 1 = 2$

2. Для $r = 2$ знаходимо Δr:

$$\Delta r = \sum_{j=0}^{L} L_j s_{r-j} = \sum_{j=0}^{1} L_j s_{2-j} = L_0 s_2 + L_1 s_1 = a^8 \cdot a^8 + a^3 \cdot a^7 = a^8 + a^2 = a^3 .$$

Оскільки $\Delta r \neq 0$, обчислимо новий многочлен зв'язків:

$M(x) = L(x) - \Delta r \cdot x \cdot B(x) = a^3 x + a^8 - a^3 \cdot x \cdot a^1 = a^3 x + a^8 - a^4 x = a^5 x + a^8$

Оскільки не виконується нерівність $2L = 1 \le (r-1) = 1$, обчислимо новий локатор помилки $L(x)$ і нормуючу добавку $B(x)$:

$L(x) = M(x) = a^5 x + a^8 = \overline{a^5 a^8}$, $B(x) = x \cdot B(x) = x \cdot a^1 = \overline{a^1 0}$.

Оскільки $r \neq 2t$ переходимо до наступної ітерації $r = r + 1 = 2$

3. Для $r = 3$ аналогічно знаходимо нову нормуючу добавку $B(x)$, новий локатор помилки $L(x)$ і L:

$B(x) = a^7 x + a^2 = \overline{a^7 a^2}$, $L(x) = a^3 x^2 + a^5 x + a^8 = \overline{a^3 a^5 a^8}$, $L = r - L = 3 - 1 = 2$.

4. Для $r = 4$ аналогічно знаходимо добавку $B(x)$, локатор помилки $L(x)$ і L:

$B(x) = a^7 x^2 + a^2 x = \overline{a^7 a^2 0}$, $L(x) = a^8 x^2 + a^8 = \overline{a^8 0 a^8}$, $L = 2$.

Оскільки $r = 2t = 4$, остаточний локатор помилки $L(x) = \overline{a^8 0 a^8} = a^8 x^2 + a^8$

3) Знаходимо корні локатора помилки $L(x)$ алгоритмом Ченя, для цього використовуючи табл. 2, 3 послідовно обчислюємо $L(a^{-j})$ для кожного $j = 1,...,q-1$. Якщо $L(a^{-j}) = 0$, то Y_j елемент кодової комбінації $Y(x)$ містить помилку.

$L(a^{-7}) = L(a^1) = a^{10} + a^8 = a^2 + a^8 = a^3 \neq 0$

$L(a^{-6}) = L(a^2) = a^{12} + a^8 = a^4 + a^8 = 0$ – помилка в Y_6

$L(a^{-5}) = L(a^3) = a^{14} + a^8 = a^6 + a^8 = a^1 \neq 0$

$L(a^{-4}) = L(a^4) = a^{16} + a^8 = a^8 + a^8 = a^4 \neq 0$

$L(a^{-3}) = L(a^5) = a^{18} + a^8 = a^2 + a^8 = a^3 \neq 0$

$L(a^{-2}) = L(a^6) = a^{20} + a^8 = a^4 + a^8 = 0$ – помилка в Y_2

$L(a^{-1}) = L(a^7) = a^{22} + a^8 = a^6 + a^8 = a^1 \neq 0$

$L(a^0) = L(a^8) = a^{24} + a^8 = a^8 + a^8 = a^4 \neq 0$

Отже, виявили, що в Y_6-му і Y_2-му елементі кодової комбінації є помилки, які відповідають $e(x)$.

4) Визначаємо характер помилки алгоритмом Форне, використовуючи табл. 2, 3. Для цього спочатку обчислюємо многочлен значень помилок $W(x)$:

$$W(x) = s(x) \cdot L(x) \bmod x^{2t} = (a^4x^3 + a^3x^2 + a^8x + a^7) \cdot (a^8x^2 + a^8) \bmod x^4$$

$$= (a^4x^5 + a^3x^4 + a^8x + a^7) \bmod x^4 = a^8x + a^7 = \overline{00a^8a^7}$$

Знаходимо похідну від $L(x)$:

$$L'(x) = (a^8x^2 + a^8)' = 2a^8x = a^4x$$

Знаходимо корегувальний поліном, для цього у формулу $e'_l = -\dfrac{W(X_l^{-1})}{L'(X_l^{-1})}$ замість X_l^{-1} підставляємо знайдені у 3 пункті степені a, при яких $L(a^{-j}) = 0$:

$$e'_6 = -\frac{W(a^{-6})}{L'(a^{-6})} = \frac{W(a^2)}{L'(a^2)} = \frac{a^{10} + a^7}{a^6} = \frac{a^2 + a^7}{a^6} = \frac{a^4}{a^6} = a^{-2} = a^6$$

$$e'_2 = -\frac{W(a^{-2})}{L'(a^{-2})} = \frac{W(a^6)}{L'(a^6)} = \frac{a^{14} + a^7}{a^{10}} = \frac{a^6 + a^7}{a^2} = \frac{a^5}{a^2} = a^3$$

Отже, корегувальний поліном $e'(x) = \overline{0a^6000a^300} = \overline{0012000000220000}$

5) Виправляємо помилки в $Y(x)$. Для цього корегувальний поліном $e'(x)$ накладаємо на $Y(x)$, використовуючи табл. 2:

$$C'(x) = Y(x) + e'(x) = \overline{a^3a^6a^8a^7a^1a^4a^3a^4} + \overline{0a^6000a^300} = \overline{a^3a^2a^8a^7a^1a^2a^3a^4} = C(x).$$

Отже, $C'(x) = C(x)$, тобто за допомогою РС-кодів (8,4) над полем Галуа GF(3^2) було виправлено 2 помилкові пари тритів. Тепер для отримання початкового інформаційного полінома відкидаємо чотири пари перевірочних тритів і отримаємо $S'(x) = \overline{a^3a^2a^8a^7} = \overline{22210111}$, що і є початковим інформаційним поліномом.

2. Дослідження корегувальної здатності трійкових РС-кодів при передачі інформації з використанням переплутаних пар кутритів квантовим каналом із шумом. При передачі інформації квантовим каналом потрібно враховувати особливості квантового шуму. Однією з основних моделей квантового шуму є модель деполяризуючого каналу [1]. Відповідно до цієї моделі, у квантовому каналі під час передачі чистий стан окремого кубіту (кудиту) з імовірністю *p* деполяризується, тобто його стан стає повністю змішаним (виникає помилка), а з імовірністю $(1-p)$ стан кубіту (кудиту) залишається незмінним. Аналогічно, при передачі кутриту, який знаходиться в переплутаному стані з іншим кутритом, деполяризація в квантовому каналі приводить до зміни всього переплутаного стану [28]. Тому, досліджувалась корегувальна здатність трійкових РС-кодів залежно від імовірності деполяризації *p*. Результати дослідження наведено у табл. 4.

Таблиця 4. Випробування корегувальної здатності РС кодів (8,4) над полем Галуа GF(3^2)

p	Кількість передаваних блоків по 8 пар тритів	Кількість переданих пар кутритів		Відсоток переданих пар кутритів без помилок	Кількість переданих блоків даних по 8 пар купритів		Відсоток переданих блоків без помилок
		без помилок	з помил-ками		без помилок	з помил-ками	
0	1000000	8000000	0	100	1000000	0	100
0,05	1000000	7600105	399895	95,0013	994179	5821	99,4179
0,1	1000000	7198339	801661	89,9792	961506	38494	96,1506
0,15	1000000	6799046	1200954	84,9880	894519	105481	89,4519
0,2	1000000	6400722	1599278	80,0090	797656	202344	79,7656
0,25	1000000	6000164	1999836	75,0020	678759	321241	67,8759
0,3	1000000	5597119	2402881	69,9639	551034	448966	55,1034
0,35	1000000	5196660	2803340	64,9582	426666	573334	42,6666
0,4	1000000	4798706	3201294	59,9838	314579	685421	31,4579
0,45	1000000	4400166	3599834	55,0020	220449	779551	22,0449
0,5	1000000	3998354	4001646	49,9794	144018	855982	14,4018
0,55	1000000	3600062	4399938	45,0007	88577	911423	8,8577
0,6	1000000	3198925	4801075	39,9865	49676	950324	4,9676
0,65	1000000	2800679	5199321	35,0084	24998	975002	2,4998
0,7	1000000	2399026	5600974	29,9878	11279	988721	1,1279
0,75	1000000	1999520	6000480	24,9940	4265	995735	0,4265
0,8	1000000	1599767	6400233	19,9970	1206	998794	0,1206
0,85	1000000	1200305	6799695	15,0038	240	999760	0,024
0,9	1000000	801655	7198345	10,0206	19	999981	0,0019
0,95	1000000	399902	7600098	4,9987	0	1000000	0
1	1000000	0	8000000	0	0	1000000	0

Імовірність деполяризації p фіксувалась на початку кожного етапу дослідження, після чого імітувалась передача інформації, попередньо закодованої трійковими РС-кодами, парами переплутаних кутритів квантовим каналом. Перебиралися всі значення p з кроком 0,01. Передавана інформація генерувалась псевдовипадковим чином у вигляді послідовності трійкових даних, які розбивались на блоки з чотирьох пар тритів. Після чого виконувалось їх кодування РС-кодами (8,4) над полем Галуа $GF(3^2)$, в результаті кожен блок розширювався до восьми пар тритів, які попарно передавались квантовим каналом. Для кожного p передавались 1000000 таких блоків. Із заданою імовірністю p імітувались помилки при передачі кожної пари тритів, при цьому значення пари тритів змінювалось випадковим чином на одне з інших восьми можливих, що відповідає зміні стану переплутаної пари кутритів внаслідок деполяризації в квантовому каналі. Після отримання блоків виконувалось їх декодування РС-кодами. Якщо при декодуванні виявлялося, що кількість помилкових пар тритів в кожному блоці не більше двох – РС-коди їх виправляли, в противному випадку декодувати блок було не можливо. Дані про кількість отриманих та виправлених помилок, кількість блоків, які були успішно декодовані і які не можливо декодувати, збиралися у вигляді статистики (див. табл. 4).

Висновки

У роботі детального розглянуто використання трійкових РС-кодів та виконано оцінку їх корегувальної здатності при передачі інформації з використанням переплутаних пар кутритів у квантовому каналі з шумом, що є актуальним для практичної реалізації квантових протоколів прямого безпечного зв'язку з кутритами. Отримана статистична інформація показує, що коди добре справляються з корекцією помилок, якщо ймовірність деполяризації кутриту в квантовому каналі не перевищує 25-30%. Оскільки в сучасних експериментах рівень помилок при передаванні фотонів квантовим каналом, як правило, не перевищує декількох процентів, то звідси можна зробити висновок, що трійкові коди Ріда-Соломона цілком придатні для завадостійкого кодування в типових квантових протоколах прямого безпечного зв'язку з передаванням кутритів. Вказане відсоткове обмеження не є критичним і може змінюватися експертним методом в залежності від умов експлуатації та інших чинників.

Список літератури

1. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг. – Москва: Мир, 2006. – 824 с.
2. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, issue 18. – 187902.
3. 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.
4. Man Zh.-X. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations / Zh.-X. Man, Zh.-J. Zhang, Y . Li // Chinese Physics Letters. – 2005. – V. 22, №1. – P.18–21.
5. 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.
6. Gao T. Quantum secure conditional direct communication via EPR pairs / T. Gao, F.-L. Yan, Zh.-X. Wang // International Journal of Modern Physics C. – 2005. – V. 16, № 8. – P. 1293–1301.
7. Wang J. Multiparty controlled quantum secure direct communication using Greenberger – Horne – Zeilinger state / J. Wang, Q. Zhang, C.J. Tang // Optics Communications. – 2006. – V. 266, № 2. – P. 732–737.
8. Gao T. Deterministic secure direct communication using GHZ states and swapping quantum entanglement / T. Gao, F.-L. Yan, Zh.-X. Wang // Journal of Physics A. – 2005. – V. 38, № 25. – P. 5761–5770.
9. Gao T. A Simultaneous quantum secure direct communication scheme between the central party and other *M* parties / T. Gao, F.-L. Yan, Zh.-X. Wang // Chinese Physics Letters. – 2005. – V. 22, № 10. – P. 2473–2476.
10. Deng F.-G. Multiparty quantum secret report / F.-G. Deng, X.-H. Li, Ch.-Y.Li, P. Zhou, Y.-J. Liang, H.-Y. Zhou // Chinese Physics Letters. – 2006. – V. 23, № 7. – P. 1676–1679.
11. Li X.-H. Multiparty quantum remote secret conference / X.-H. Li, Ch.-Y. Li, F.-G. Deng, P. Zhou, Y.-J. Liang, H.-Y. Zhou // Chinese Physics Letters. – 2007. – V. 24, № 1. – P. 23–26.
12. 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.
13. Василиу Е.В. Анализ безопасности пинг – понг протокола с квантовым плотным кодированием / Е.В. Василиу // Наукові праці ОНАЗ ім. О.С. Попова. – 2007. – № 1. – С. 32–38.
14. 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.
15. Василиу Е.В. Оценки вычислительной сложности неквантового способа усиления безопасности пинг – понг протокола / Е.В. Василиу // Прикладная радиоэлектроника. – 2009. – № 3. – С. 396–404.
16. Gao W.-B. Experimental demonstration of a hyper – entangled ten – qubit Schrodinger cat state / W.-B. Gao, C.-Y. Lu, X.-C. Yao et al. // Nature Physics. – 2010. – V. 6. – P. 331–335.
17. Wang Ch. Quantum secure direct communication with high dimension quantum superdense coding / Ch. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, G. L. Long // Physical Review A. – 2005. – V. 71, № 4. – 044305.
18. 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.
19. Thew T. Experimental realization of entangled qutrits for quantum communication / T. Thew, A. Acin, H. Zbinden, N. Gisin // Quantum Information and Computation. – 2004. – V. 4, № 2. – P. 93–101.
20. Vaziri A. Concentration of higher dimensional entanglement: qutrits of photon orbital angular momentum / A. Vaziri, J. Pan, T. Jennewein, G. Weihs, A. Zeilinger // Physical Review Letters. – 2003. – V. 91, № 22. – 227902.
21. Вернер М. Основы кодирования: учебник для ВУЗов / М. Вернер. – Москва: Техносфера, 2004. – 288 с.

22. Жураковський Ю.П. Теорія інформації та кодування: підручник / Ю.П. Жураковський, В.П. Полторак. – К.: Вища школа, 2001. – 255 с.

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

24. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – Москва: Техносфера, 2005. – 320 с.

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

26. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Бернард Скляр. – М.:Издательский дом Вильямс, 2003. – 1104 с.

27. Котенко В.В. Теория информации и защита телекоммуникации: монография / В.В. Котенко, К.Е. Румянцев. – Ростов н/Д: Изд-во ЮФУ, 2009. – 369 с.

28. Корченко О.Г. Імітаційна модель пінг-понг протоколу з парами переплутаних кутритів у квантовому каналі з шумом / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк, В.М. Кінзерявий // Науково-технічний журнал «Захист інформації». – 2010, № 3. – С. 46–56.

Рецензент: Шелест М.Є.
Надійшла 10.11.2010