

## КЛАСИЧНА ПРОПУСКНА ЗДАТНІСТЬ КВАНТОВИХ КАНАЛІВ ЗВ'ЯЗКУ ЗА РІЗНИХ МОДЕЛЕЙ ЗАВАД У КАНАЛАХ

*Vasiliu Є.В., Гаджієв М.М., Горицький В.М., Кільдішев В.Й., Лімарь І.В.*

*Одеська національна академія зв'язку ім. О.С. Попова,  
65029, Україна, м. Одеса, вул. Кузнечна, 1.  
[vasiliu@te.net.ua](mailto:vasiliu@te.net.ua)*

## КЛАССИЧЕСКАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ КВАНТОВЫХ КАНАЛОВ СВЯЗИ ПРИ РАЗЛИЧНЫХ МОДЕЛЯХ ПОМЕХ В КАНАЛАХ

*Василиу Е.В., Гаджиев М.М., Горицкий В.М., Кильдишев В.И., Лимарь И.В.*

*Одесская национальная академия связи им. А.С. Попова,  
65029, Украина, г. Одесса, ул. Кузнечная, 1.  
[vasiliu@te.net.ua](mailto:vasiliu@te.net.ua)*

## CLASSICAL TRANSMISSION CAPACITY OF QUANTUM COMMUNICATION CHANNELS IN VARIOUS MODELS OF NOISE IN CHANNELS

*Vasiliu YE.V., Gadzhiev M.M., Horyts'kyi V.M., Kildishev V.Y., Limar I.V.*

*O.S. Popov Odessa national academy of telecommunications,  
1 Kuznechna St., Odessa, 65029, Ukraine.  
[vasiliu@te.net.ua](mailto:vasiliu@te.net.ua)*

**Анотація.** Одержані аналітичні вирази для класичної пропускної здатності квантових каналів за різних моделей завад: деполаризувального каналу, каналу із загасанням амплітуди та каналу із загасанням фази при кодуванні інформації базисними станами кубіту та кутриту. Показано, що класична пропускна здатність розглянутих квантових каналів вище пропускної здатності відповідних класичних каналів зв'язку. Отримані у роботі результати можуть бути використані при побудові ефективних завадостійких кодів, які необхідні для практичної реалізації протоколів квантової криптографії.

**Ключові слова:** квантові канали зв'язку, пропускна здатність, кубіт, кутрит, матриця щільності, деполаризувальний канал, канал із загасанням амплітуди, канал із загасанням фази.

**Аннотация.** Получены аналитические выражения для классической пропускной способности квантовых каналов в разных моделях помех: деполаризующего канала, канала с затуханием амплитуды и канала с затуханием фазы при кодировании информации базисными состояниями кубита и кутрита. Показано, что классическая пропускная способность рассмотренных квантовых каналов выше пропускной способности соответствующих классических каналов связи. Полученные в работе результаты могут быть использованы при построении эффективных помехоустойчивых кодов, необходимых для практической реализации протоколов квантовой криптографии.

**Ключевые слова:** квантовые каналы связи, пропускная способность, кубит, кутрит, матрица плотности, деполаризующий канал, канал с затуханием амплитуды, канал с затуханием фазы.

**Abstract.** Analytical expressions for classical transmission capacity of quantum channels in various models of noise are derived, namely for the depolarizing channel, for the channels with amplitude and phase damping, when coding information by basic states of qubit and qutrit. It is shown that classical transmission capacity of the considered quantum channels is higher than transmission capacity of the corresponding classical communication channels. The obtained results can be used for construction of effective error-correcting codes, necessary for realization of quantum cryptography protocols.

**Key words:** quantum communication channels, transmission capacity, qubit, qutrit, density matrix, depolarizing channel, channel with amplitude damping, channel with phase damping.

В останні роки методи квантової криптографії знаходять все більш широке застосування в галузі захищеного зв'язку. На ринку засобів захисту з'являються пристрої передавання інформації окремими фотонами, які використовуються для передавання секретного ключа. У той самий час розроблено достатньо значну кількість квантових протоколів для безпечного передавання не тільки секретного ключа, але й безпосередньо конфіденційних даних (без шифрування) шляхом передавання окремих фотонів або їхніх невеликих груп. Один з таких протоколів, в якому дані передаються окремими фотонами – кубітами, запропоновано авторами [1]. Відзначимо, що на даний час розроблено способи генерації квантових фотонних систем розмірності більше двох – кутритів, куквартів тощо [2]. Протокол [1] може бути узагальнений на використання таких квантових систем високої розмірності, що дозволить підвищити швидкість передавання.

Однією з основних характеристик квантових каналів з завадами є їх пропускна здатність. На відміну від звичайного класичного каналу, який має одну пропускну здатність, квантові канали мають їх декілька, наприклад, класична пропускна здатність квантового каналу, квантова пропускна здатність квантового каналу тощо [3]. Для протоколів квантової криптографії основний інтерес являє собою класична пропускна здатність квантових каналів.

**Метою даної статті** є розрахунок класичної пропускну здатності каналів з передаванням кубітів та кутритів для різних моделей шуму.

Однією з основних моделей квантового шуму, яка багато використовується на даний час у квантовій теорії інформації, є модель деполяризувального каналу. Для чистого стану одиночного кубіту дія цього каналу полягає в наступному: з імовірністю  $p$  цей кубіт деполяризується, тобто його стан стає повністю змішаним, а з імовірністю  $(1 - p)$  стан кубіту залишається незмінним. Оператор деполяризувального каналу для кубітів може бути представлений у вигляді [4]:

$$\varepsilon(\rho) = (1 - p)\rho + \frac{p}{3}(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z), \quad (1)$$

де  $\rho$  – оператор щільності кубіту;  $\sigma_x$ ,  $\sigma_y$  та  $\sigma_z$  – оператори Паулі.

Оператор деполяризувального каналу, який діє на чистий стан окремого кутриту, має вигляд [5]:

$$\varepsilon_{\text{qurit}}(\rho) = (1 - p)\rho + \frac{p}{8}(Y\rho Y^\dagger + Z\rho Z^\dagger + Y^2\rho(Y^2)^\dagger + YZ\rho(YZ)^\dagger + Y^2Z\rho(Y^2Z)^\dagger + YZ^2\rho(YZ^2)^\dagger + Y^2Z^2\rho(Y^2Z^2)^\dagger + Z^2\rho(Z^2)^\dagger), \quad (2)$$

де  $\rho$  – оператор щільності кутриту, а матриці  $Y$  та  $Z$  мають вигляд:

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

Дві інші значно відомі моделі квантових каналів з завадами: канал із загасанням амплітуди (дисипацією енергії) та канал із загасанням фази (процес, за якого фотони випадково розсіюються при їх поширенні хвилеводом) [4,5]. Ці канали можуть бути описані супер-оператором  $\Phi$  у зображенні операторів Крауса:

$$\rho_\Phi = \Phi\rho = \sum_k E_k\rho E_k^\dagger, \quad (4)$$

де  $\rho_\Phi$  – матриця щільності кубіту, кутриту або квантової системи більшої розмірності на виході каналу.

Для каналу із загасанням амплітуди матриці  $E_k$  мають такий вигляд:

для кубітів [4]:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{pmatrix}, \quad (5)$$

для кутритів [5]:

$$E_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{1-\lambda} & 0 \\ 0 & 0 & \sqrt{1-\lambda} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sqrt{\lambda} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, E_2 = \begin{pmatrix} 0 & 0 & \sqrt{\lambda} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad (6)$$

де  $\lambda$  – деякий параметр помилки.

Для каналу із загасанням фази:

для кубітів [4]:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\varepsilon} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\varepsilon} \end{pmatrix}, \quad (7)$$

для кутритів [5]:

$$E_0 = \sqrt{1-\varepsilon} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, E_1 = \sqrt{\varepsilon} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad (8)$$

де  $\varepsilon$  – ймовірність помилки;  $\omega = e^{2\pi i/3}$ .

У випадку кодування бітів (третів, ...) ортогональними квантовими станами та виконання вимірювань на приймальній стороні в тих самих базисах, що використовувались для кодування, класична пропускна здатність квантового каналу описується тією ж формулою, що й звичайна пропускна здатність класичного каналу зв'язку [3]:

$$C = \max_{P(x_j)} \sum_j \sum_i P(x_j) P(y_i | x_j) \log [P(y_i | x_j) / P(y_i)], \quad (9)$$

де  $x_j$  та  $y_i$  – вхідні та вихідні символи каналу відповідно.

Підставляючи в (1) – (4) матриці щільності кубіту та кутриту на передавальній стороні:

$$\rho^{(qubit)} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{pmatrix}, \rho^{(qutrit)} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* & \alpha\gamma^* \\ \beta\alpha^* & |\beta|^2 & \beta\gamma^* \\ \gamma\alpha^* & \gamma\beta^* & |\gamma|^2 \end{pmatrix} \quad (10)$$

та використовуючи (5) – (8), можна одержати відповідні матриці щільності на приймальній стороні для різних моделей каналів.

Так, для деполаризувального каналу одержимо:

$$\rho_{\Phi(depol)}^{(qubit)} = \begin{pmatrix} (1-2p/3)|\alpha|^2 + 2p/3|\beta|^2 & (1-4p/3)\alpha\beta^* \\ (1-4p/3)\beta\alpha^* & (1-2p/3)|\beta|^2 + 2p/3|\alpha|^2 \end{pmatrix},$$

$$\rho_{\Phi(depol)}^{(qutrit)} = \frac{1}{8} \begin{pmatrix} (3p(|\beta|^2 + |\gamma|^2) + (8-6p)|\alpha|^2) & (8-9p)\alpha\beta^* & (8-9p)\alpha\gamma^* \\ (8-9p)\beta\alpha^* & (3p(|\alpha|^2 + |\gamma|^2) + (8-6p)|\beta|^2) & (8-9p)\beta\gamma^* \\ (8-9p)\gamma\alpha^* & (8-9p)\gamma\beta^* & (3p(|\alpha|^2 + |\beta|^2) + (8-6p)|\gamma|^2) \end{pmatrix}. \quad (11)$$

Для каналу із загасанням амплітуди матриці щільності на приймальній стороні мають вигляд:

$$\rho_{\Phi(dissip)}^{(qubit)} = \begin{pmatrix} |\alpha|^2 + \lambda|\beta|^2 & \sqrt{1-\lambda}\alpha\beta^* \\ \sqrt{1-\lambda}\beta\alpha^* & \sqrt{1-\lambda}|\beta|^2 \end{pmatrix},$$

$$\rho_{\Phi(dissip)}^{(qutrit)} = \begin{pmatrix} |\alpha|^2 + \lambda(|\beta|^2 + |\gamma|^2) & \sqrt{1-\lambda}\alpha\beta^* & \sqrt{1-\lambda}\alpha\gamma^* \\ \sqrt{1-\lambda}\beta\alpha^* & (1-\lambda)|\beta|^2 & (1-\lambda)\beta\gamma^* \\ \sqrt{1-\lambda}\gamma\alpha^* & (1-\lambda)\gamma\beta^* & (1-\lambda)|\gamma|^2 \end{pmatrix}. \quad (12)$$

Нарешті, для каналу із загасанням фази:

$$\rho_{\Phi(dephas)}^{(qubit)} = \begin{pmatrix} |\alpha|^2 & \sqrt{1-\varepsilon}\alpha\beta^* \\ \sqrt{1-\varepsilon}\beta\alpha^* & |\beta|^2 \end{pmatrix},$$

$$\rho_{\Phi(dephas)}^{(qutrit)} = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* & \alpha\gamma^* \\ \beta\alpha^* & |\beta|^2 & \beta\gamma^* \\ \gamma\alpha^* & \gamma\beta^* & |\gamma|^2 \end{pmatrix}. \quad (13)$$

Як видно з (13), для каналу із загасанням фази для кутритів матриці щільності на вході та виході каналу однакові, а для кубітів ці матриці відрізняються тільки недіагональними елементами. Це означає, що канал із загасанням фази дозволяє безпомилково передавати класичну інформацію шляхом її кодування базисними станами, що узгоджується з відомими результатами інших авторів [6].

Максимального значення величина (9) досягає, коли всі  $P(x_j)$  та  $P(y_i)$  рівні між собою, тобто для кубітів всі вони дорівнюють 1/2, а для кутритів – 1/3. Перехідні ймовірності  $P(y_i | x_j)$  для деполяризувального каналу та каналу із загасанням амплітуди обчислюються з використанням матриць (11), (12). Тоді, підставляючи одержані ймовірності в (9), одержимо відповідні пропускні здатності (у бітах на символ).

Таким чином, класична пропускна здатність деполяризувального каналу:

$$C_{depol}^{(qubit)}(p) = 1 + \left(1 - \frac{2p}{3}\right) \log_2 \left(1 - \frac{2p}{3}\right) + \frac{2p}{3} \cdot \log_2 \left(\frac{2p}{3}\right),$$

$$C_{depol}^{(qutrit)}(p) = \log_2 3 + \left(1 - \frac{3p}{4}\right) \log_2 \left(1 - \frac{3p}{4}\right) + 2 \cdot \frac{3p}{8} \cdot \log_2 \left(\frac{3p}{8}\right). \quad (14)$$

Зазначимо, що  $p$  в (12) – це ймовірність деполяризації кубіта або кутрита. Ця величина не дорівнює ймовірності помилки, оскільки, як відомо [4], деполяризація не завжди призводить до помилки.

Класична пропускна здатність каналу із загасанням амплітуди:

$$C_{ampl}^{(qubit)}(\lambda) = 1 + \frac{1}{2}(1-\lambda) \log_2(1-\lambda) + \frac{1}{2}\lambda \log_2 \lambda,$$

$$C_{ampl}^{(qutrit)}(\lambda) = \frac{\log_2 3}{3} + \frac{2\lambda}{3} \log_2(3\lambda) + \frac{2}{3}(1-\lambda) \log_2(3(1-\lambda)). \quad (15)$$

На рис. 1 представлені залежності від ймовірності деполяризації  $p$  величин (14). Крива 1 відповідає каналу з передаванням одиночних кутритів, крива 2 – з передаванням одиночних кубітів. На рис. 2 представлені залежності від ймовірності помилки  $\lambda$  класичної пропускної здатності каналу із загасанням амплітуди (15). Крива 1 відповідає каналу з кутритами, крива 3 – каналу з кубітами. Також на рис. 2 для порівняння показані пропускні здатності відповідних класичних каналів – тритового (крива 2) та бітового (крива 4). Як видно, класична пропускна здатність квантового каналу із загасанням фази більше пропускної здатності класичного каналу. Зазначимо, що це твердження справедливе також для деполяризувального квантового каналу.

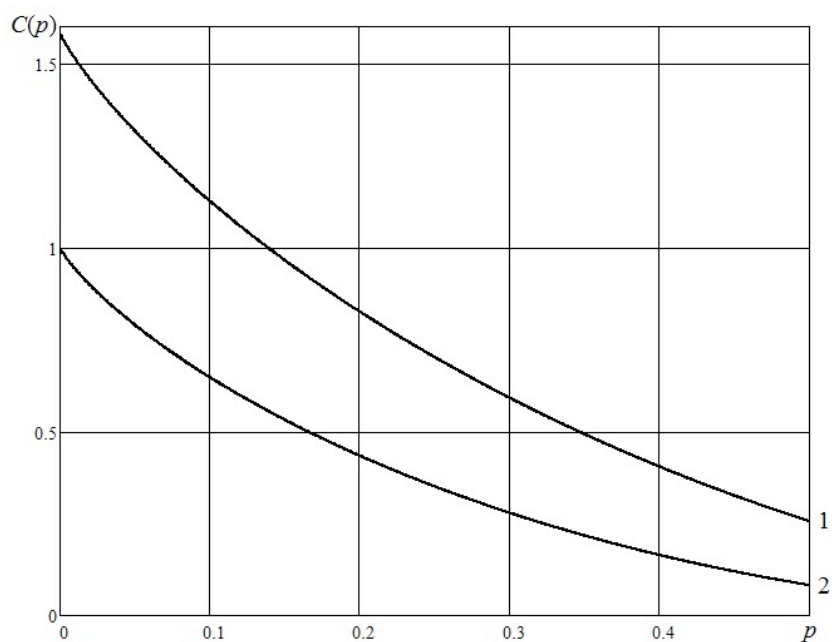


Рисунок 1 – Класична пропускна здатність квантового деполаризувального каналу

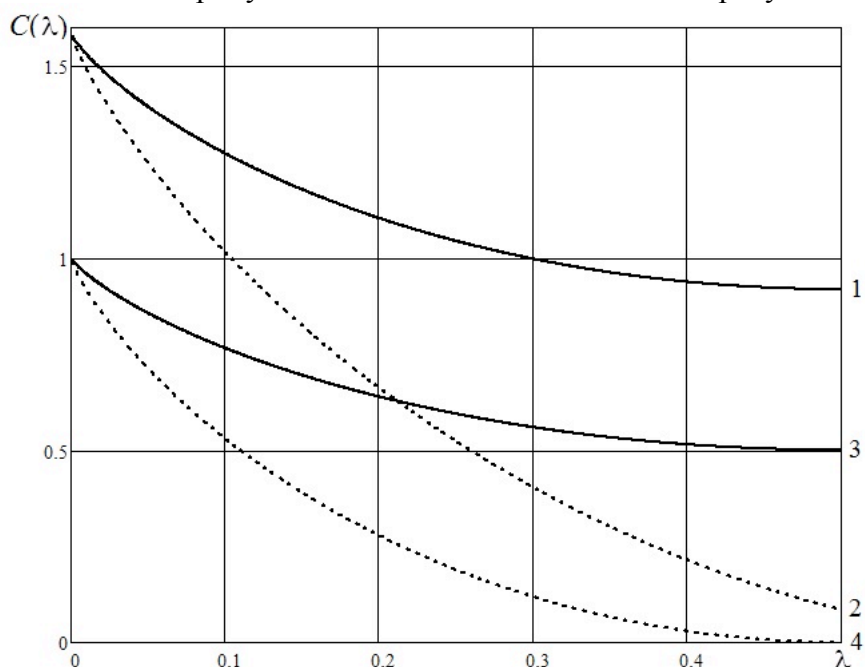


Рисунок 2 – Класична пропускна здатність квантового каналу із загасанням амплітуди

У роботі одержані аналітичні вирази для класичної пропускної здатності деполаризувального квантового каналу, каналів із загасанням амплітуди та фази при кодуванні інформації базисними станами кубіту та кутриту. Показано, що класична пропускна здатність зазначених квантових каналів вище пропускної здатності відповідних класичних каналів зв'язку. Отримані результати для пропускної здатності квантових каналів можуть бути використані для побудови ефективних завадостійких кодів, які також повинні враховувати особливості передавання інформації у конкретному протоколі квантової криптографії.

Публікація містить результати досліджень, проведених за грантової підтримки Держаного фонду фундаментальних досліджень України за конкурсним проектом (договір № Ф73/91-2016).

ЛІТЕРАТУРА:

1. Барановский О.К. Многоканальная квантовая система волоконно-оптической безопасной связи / Барановский О.К., Гулаков И.Р., Василиу Е.В., Зеневич А.О., Лимарь И.В. // Научно-практический журнал "Безпека інформації". – 2016. – Т. 22. – № 2. – С. 156–162.
2. Bogdanov Yu. I. Qutrit state engineering with biphotons / Yu. I. Bogdanov, M.V. Chekhova, S. P. Kulik et al. // Physical Review Letters. – 2004. – V. 93. – 230503.
3. Холево А.С. Квантовые системы, каналы, информация / Холево А.С. – М.: МЦНМО, 2010. – 328 с.
4. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг – М.: Мир, 2006. – 824 с.
5. Ramzan M. Noisy non-transitive quantum games / M. Ramzan, S. Khan, M.K. Khan // Journal of Physics A: Mathematical and Theoretical. – 2010. – V. 43, N. 26. – 265304.
6. Grassl M. Quantum Error Correction / Grassl M. // Lectures on Quantum Information / Bruss D., Leuchs G. (eds.). – Weinheim: WILEY-VCH Verlag, 2007. – 610 p.

REFERENCES:

1. Baranovsky O. Multichannel quantum system of fiber-optics secure communication / Baranovsky O., Gulakov I., Vasiliu Ye., Zenevich A., Limar I. // Ukrainian Scientific Journal of Information Security. – 2016. – V. 22, N 2. – P. 156–162.
2. Bogdanov Yu. I. Qutrit state engineering with biphotons / Yu. I. Bogdanov, M.V. Chekhova, S. P. Kulik et al. // Physical Review Letters. – 2004. – V. 93. – 230503.
3. Holevo A.S. Quantum systems, channels, information / Holevo A.S. – М.: MCNMO, 2010. – 328 p.
4. Nielsen M. Quantum Computation and Quantum Information / Nielsen M., Chuang I. – М.: Mir, 2006. – 824 p.
5. Ramzan M. Noisy non-transitive quantum games / M. Ramzan, S. Khan, M.K. Khan // Journal of Physics A: Mathematical and Theoretical. – 2010. – V. 43, N 26. – 265304.
6. Grassl M. Quantum Error Correction / Grassl M. // Lectures on Quantum Information / Bruss D., Leuchs G. (eds.). – Weinheim: WILEY-VCH Verlag, 2007. – 610 p.