DOI: 10.18372/2310-5461.46.14803

УДК 621.3(045)

***Б. О. Білаш***
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»
orcid.org/0000-0002-1341-1920
e-mail: bogdanbelash35@gmail.com

# МОДИФІКОВАНИЙ МЕТОД КОРЕКЦІЇ ПОМИЛОК ІЗ ЗАСТОСУВАННЯМ ШИФРУ ВЕРНАМА У СИСТЕМАХ QKD

**Вступ**

Відомо, що квантове розповсюдження ключів (Quantum Key Distribution, QKD) є методом надійної передачі захищеного ключа між двома віддаленими сторонами в сучасній криптографії [1]. На відміну від відомих класичних криптографічних протоколів, таких як RSA (Rivest – Shamir – Adleman), який ґрунтується на практичній складності факторизації перемноження двох великих простих чисел [2], метод QKD заснований на створенні справді випадкових ключів.

**Постановка проблеми**

Відомо, що наразі область квантової криптографії інтенсивно розвивається в системах квантового розповсюдження ключів. Системи QKD мають як переваги, зокрема, створення справді випадкового ключа, забезпеченого законами квантової фізики, так і недоліки, наприклад, помилки, які виникають із-за шумів у ненадійному квантовому каналі та аномалій, викликаних третьою стороною, які знижають його надійність.

Наразі розвиваються два напрямки підвищення надійності систем QKD: дослідження квантового каналу на фізичному рівні та дослідження виправлення помилок після створення просіяного ключа. Саме тому розробка нових та удосконалення існуючих методів і засобів виявлення та усунення помилок у системах QKD наразі є важливим та актуальним завданням.

**Аналіз останніх досліджень і публікацій**

Перший протокол BB84 [3] для реалізації методу QKD був запропонований ще у 1984 р., цей напрям у сучасній науці продовжує активно досліджуватися та розвиватися.

Як приклад науково-дослідних робіт за тематикою QKD можна привести роботи по розробленню систем зменшення розмірів мікросхем [4], комунікацій на великі відстані [5], високої та безпечної швидкості передачі ключа QKD [6]–[8], проведення ефективної пост-обробки [9] тощо.

Основне завдання пост-обробки полягає у виправленні помилок, щоб поділитися однаковим захищеним ключем між двома сторонами (які, зазвичай, звуться Алісою та Бобом). Їх причиною можуть бути різні фактори. Ненадійність квантового каналу зумовлена тим, що фотони можуть викликати шум при зміні вектора поляризації фотона. Помилки можуть також виникати під час прийому фотонів Бобом і неправильного читання стану фотона. Одиночний детектор фотонів, який є надзвичайно чутливою складовою для виявлення одиночного фотона, також має деякі шуми такі як Dark count, After pulse, але найвагоміший вплив спричиняє шум в оптичному каналі під назвою Cross talk [10]. Чарльз Беннет та Жиль Бассард показали, що якщо коефіцієнт квантових бітових помилок QBER (quantum bit error rate) в каналі не перевищує 11 %, то скоріш за все це зумовлено впливом саме шумів, а не аномалій, викликаних впливом третьої сторони (яку, зазвичай, називають Євою). Зазвичай, показник рівня бітових помилок QBER при середньому рівні шумів в системі становить не більше 5 %. Саме виправлення помилок за рахунок шумів, які виникли під час фази обміну фотонами і є основним завданням на етапі пост-обробки. Нижче зупинимось на розгляді існуючих підходів корекції помилок в квантовому каналі.

Дана робота базується на роботі Маріо Міліцевіча в області CV-QKD (continuous variable QKD), про яку розповідатиметься далі.

М. Міліцевич запропонував надійний метод корекції помилок, але CV-QKD системи, де Аліса кодує свою інформацію в амплітудній та фазовій квадратурах когерентних станів, є досі не надто розповсюдженими. Тому виникає питання про адаптацію метода Міліцевича до DV-QKD систем, де Аліса кодує свою інформацію в поляризації однофотонних станів.

**Мета**

Дослідження методів виправлення помилок у системах квантового розподілу ключів (QKD). QKD — це система, яка використовує фотони та

закони квантової фізики для створення ключа шифрування, який використовується в сучасній криптографії. На відміну від сучасних класичних криптографічних протоколів, протокол QKD заснований на створенні справді випадкових ключів, які можна використовувати в одноразових блокнотах, які мають властивість абсолютної криптографічної стійкості.

**Аналіз існуючих методів виправлення помилок**

Наразі існує декілька популярних підходів, які використовуються для виправлення квантових бітових помилок, зокрема, такі методи як Cascade, Winnow та LDPC (low density parity check) із застосуванням кодів перевірки парності низької щільності [11–15]. Ідеї, покладені в їх основу, запозичені з класичних методів корекції помилок.

При реалізації методу Cascade [11] у кожному проході Аліса та Боб домовляються про випадкову перестановку, яка стосується їхніх бітів.

При реалізації методу Winnow [12], як і методу Cascade, здійснюється поділ двійкових рядків на блоки, але замість виправлення помилок за допомогою ітеративної бінарної фіксації метод базується на використанні кодів Хеммінга.

Однак, обидва зазначених вище методів не є ефективними при роботі з повідомленнями великої довжини, а також при передачі повідомлень на великі відстані. Виникає потреба у використанні підходу, який би містив контрольні біти разом з основним повідомленням за один раз під час транспортування.

Шляхом усунення вказаних вище недоліків є застосування методу виправлення помилок LDPC [13]. У свій час він не отримав належної уваги з боку дослідників через занадто високі вимоги до обчислювальних потужностей обладнання для його реалізації, однак, наразі, ці обмеження вже усунено. При цьому значний вклад у розвиток методу LDPC внесли відомі фахівці Девід Маккей та Редфорд Ніл [14; 15].

Розглянемо особливості реалізації методу корекції помилок LDPC в системах QKD.

Нижче на рис. 1 наведено загальний вигляд поетапної реалізації методу передачі захищеного ключа QKD.


Рис. 1. Загальний вигляд поетапної реалізації методу передачі захищеного ключа QKD

На етапі виправлення помилок Аліса та Боб мають просіяні ключі, але вони трохи відрізняються один від одного через вплив фонових шумів в системі QKD.

***Мета*** цього етапу — узгодити просіяні ключі таким чином, щоб вони були однаковими, а потім перейти до наступного етапу посилення конфіденційності. Основна проблема на цьому етапі полягає в тому, що при передачі просіяних ключів між Алісою та Бобом необхідно їх захистити, щоб третя сторона-підслуховувач (*eavesdropper*) Єва не змогла отримати просіяний ключ. Щоб уникнути цього, можна використовувати протоколи хешування для захисту інформації, що передається. Однак такий підхід є нераціональним через збільшення обчислювальних ресурсів та часу на обробку хеш-функції. Саме тому існує інший підхід до виправлення помилок та захисту інформації від Єви.

Наразі існують дві основні технології передачі ключа в системах QKD: Continuous-Variable QKD (CV-QKD), де Аліса кодує свою інформацію в амплітудній та фазовій квадратурах когерентних станів та Discrete-Variable QKD (DV-QKD), де Аліса кодує свою інформацію в поляризації однофотонних станів. В останні роки все більше уваги приділяється саме технології DV-QKD через дискретну природу поляризації фотонів, що полегшує переведення стану фотонів в біти, зменшує відсоток виникнення помилок, а також дозволяє збільшити швидкість передачі інформації.

В 2017 р. Mario Milicevic, Chen Feng, Lei M. Zhang та P. Glenn Gulak у своїй праці [16] запропонували метод та алгоритм, згідно з яким Бобом генерується випадкове повідомлення S, яке кодується в кодове повідомлення C. Після цього створюється та посилається до Аліси класичне повідомлення M, модулюючи кодове слово C з корельованою гаусовою послідовністю Y. Після отримання повідомлення M Аліса проводить зворотну операцію обчислення повідомлення M з корельованою гаусовою послідовністю X, отримуючи вектор R.

Після цього вектор R декодується та отримується повідомлення $\hat{S}$, яке має дорівнювати повідомленню S. Однак у праці [16] авторами використовується технологія CV-QKD, а вектори X та Y є корельованими гаусовими послідовностями.

Оскільки для проведення дослідження із врахуванням зазначених вище переваг обрано більш перспективну технологію DV-QKD, в рамках даної роботи передбачено адаптацію наведеного вище в [16] методу та алгоритму для застосування в DV-QKD системах.

**Шифр Вернама**

Представлення векторів X та Y у вигляді корельованих гаусових послідовностей для реалізації в технології DV-QKD не є прийнятним, оскільки ці вектори мають бути дискретними. Тому необхідно знайти спосіб їх представлення в DV-QKD. Також обробка модулювання повідомлень корельованими гаусовими послідовностями потребує використання великих комп'ютерних ресурсів, часу обробки та розроблення відповідного алгоритму. Також необхідно знайти більш просте рішення для обчислення кодового слова зі свіжим ключем.

Саме таке рішення запропоновано автором в даній роботі. Оскільки тут застосовується технологія DV-QKD замість CV-QKD, після обміну фотонами та узгодженням довжини й позицій фотонів Аліса і Боб переводять їх в класичні біти "0" та "1", що позбавляє збереження сирих ключів у вигляді корельованих гаусових послідовностей. Після цього починається етап корекції помилок. Однак, перш ніж пояснити сутність запропонованого підходу, слід акцентувати увагу на відомий шифр Вернама [17], який знадобиться при реалізації модифікованого методу корекції. Згідно з роботою [17] для утворення шифртексту повідомлення об'єднується операцією XOR з ключем (названим «одноразовим блокнотом» або шифроблокнотом). При цьому ключ повинен мати три критично важливі властивості:

– бути справді випадковим;
– збігатися за розміром за заданим відкритим текстом;
– застосовуватися тільки один раз.

У 1949 р. Клод Шеннон написав працю [18], у якій довів абсолютну криптографічну стійкість шифру Вернама. Інших шифрів з цією властивістю не існує. Але ця властивість забезпечується лише за умови використання випадкового ключа, довжина якого дорівнює довжині повідомлення. Це обмеження робило використання шифру недоцільним, оскільки для обміну ключами обидві сторони мають передати по захищеному каналу зв'язку об'єм інформації, який дорівнює повідомленню (за наявності такого каналу доцільніше одразу передати саме повідомлення). Але наразі телекомунікаційні можливості дозволяють досить швидко передавати повідомлення різної довжини [19], отже, використання шифру Вернама викликає інтерес.

**Модифікований метод корекції помилок та алгоритм його реалізації**

Автором цієї роботи запропоновано використання просіяних ключів Аліси та Боба не для їх погодження і наступного використання на етапі

посилення конфіденційності, а в якості ключа із застосуванням шифру Вернама для узгодження повідомлення, яке надалі і буде використовуватися для підсилення конфіденційності.

На рис. 2 наведено алгоритм реалізації запропонованого рішення на етапі корекції помилок.


Рис. 2. Алгоритм реалізації запропонованого рішення на етапі корекції помилок

Розглянемо детальніше запропонований алгоритм.

*1.* Боб за допомогою генератора випадкових чисел генерує повідомлення S довжиною *N*/2.

Аліса та Боб мають згенеровані випадковим чином просіяні ключі $X_0$ та $Y_0$ певної довжини. Пропонується скорочення кількості бітів до певної однакової фіксованої довжини *N*. Це будуть нові вектори X та Y. Розглянемо детальніше запропонований алгоритм: Боб, за допомогою генератора справді випадкових чисел генерує повідомлення S довжини *N*/2.

*2.* За допомогою методу виправлення помилок LDPC Боб перетворює повідомлення S в кодове слово C. Остання половина бітів кодового слова є повідомленням S.

*3.* Далі за допомогою логічної операції XOR між векторами C та Y Боб готує повідомлення M для відправлення його Алісі.

*4.* Боб відправляє повідомлення M до Аліси, яка приймає його.

*5.* Аліса застосовує операцію XOR з векторами M та X для отримання вектору R.

*6.* Оскільки операція XOR є однаковою в обох напрямках, вектори R та C мають бути абсолютно однаковими, але вони будуть різними в тих позиціях, де відрізняються вектори X та Y (класичний аутентичний канал для передачі інформації є абсолютно надійним). На прикладі знизу дійсно видно, що в тих позиціях, де відрізняються вектори X та Y також відрізняються і вектори C та R.

*7.* Аліса застосовує корекцію помилок за допомогою методу LDPC для отримання вектору D. Після корекції помилок цей вектор є абсолютно таким, як кодове слово C.

*8.* Аліса рахує кількість бітів, які є відмінними між векторами R та D. Після цього вона ділить кількість цих бітів на загальну кількість бітів N.

Отримане значення є коефіцієнтом помилок. Якщо його значення не перевищує 11 %, то можна вважати, що Єва не здійснює підслуховування. Саме тому цей етап є найбільш важливим.

*9.* Аліса декодує вектор D та знаходить повідомлення Ŝ, яке є абсолютно ідентичним оригінальному повідомленню S у Боба. Ці обидва вектори передаються на наступний етап уже для посилення конфіденційності.

**Приклад реалізації застосованого алгоритму**

Нижче наводиться приклад роботи запропонованого алгоритму корекції помилок. При цьому слід зауважити, що LDPC-матриця генерується методом, запропонованим Девідом Маккеєм та Редфордом Нілом у працях [14; 15].

1. Нові вектори X та Y фіксованої довжини N = 40. Червоним кольором помічені біти, які відрізняються.

2. Генерація вектору S довжиною N/2 = 20.

3. Генерація вектору C. Остання половина бітів кодового слова є вектором S.

4. Отримання вектору M для відправлення його Алісі.

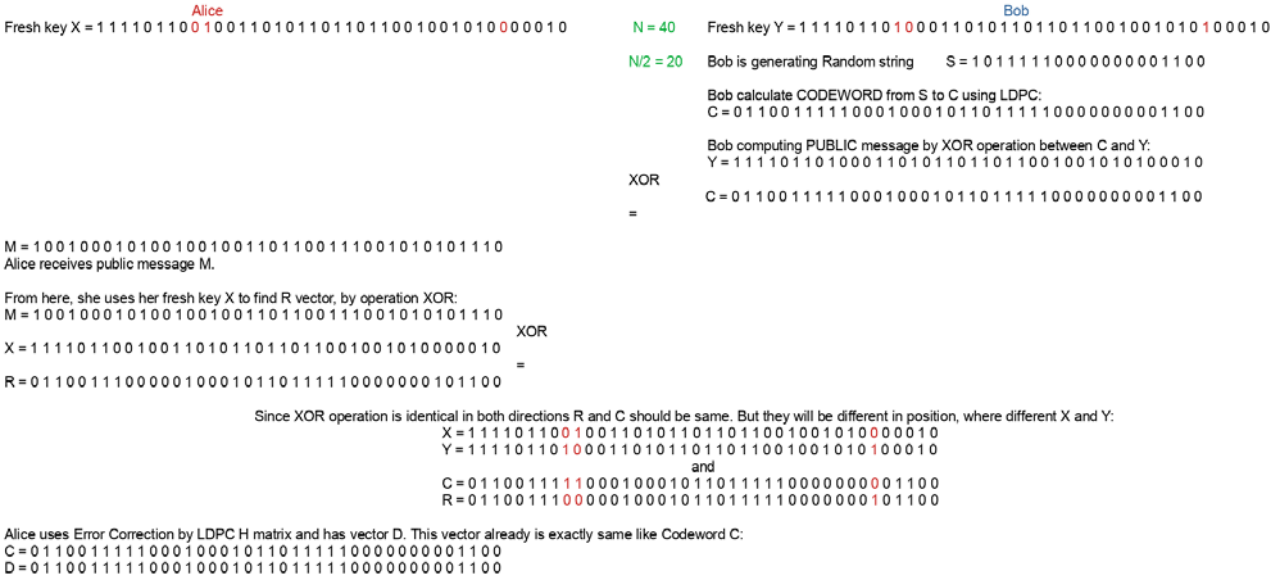
5. Отримання Алісою вектору M.

6. Генерація Алісою вектору R.

Позиції, на яких відрізняються вектори X та Y, а також вектори C та R співпадають (виділено червоним кольором).

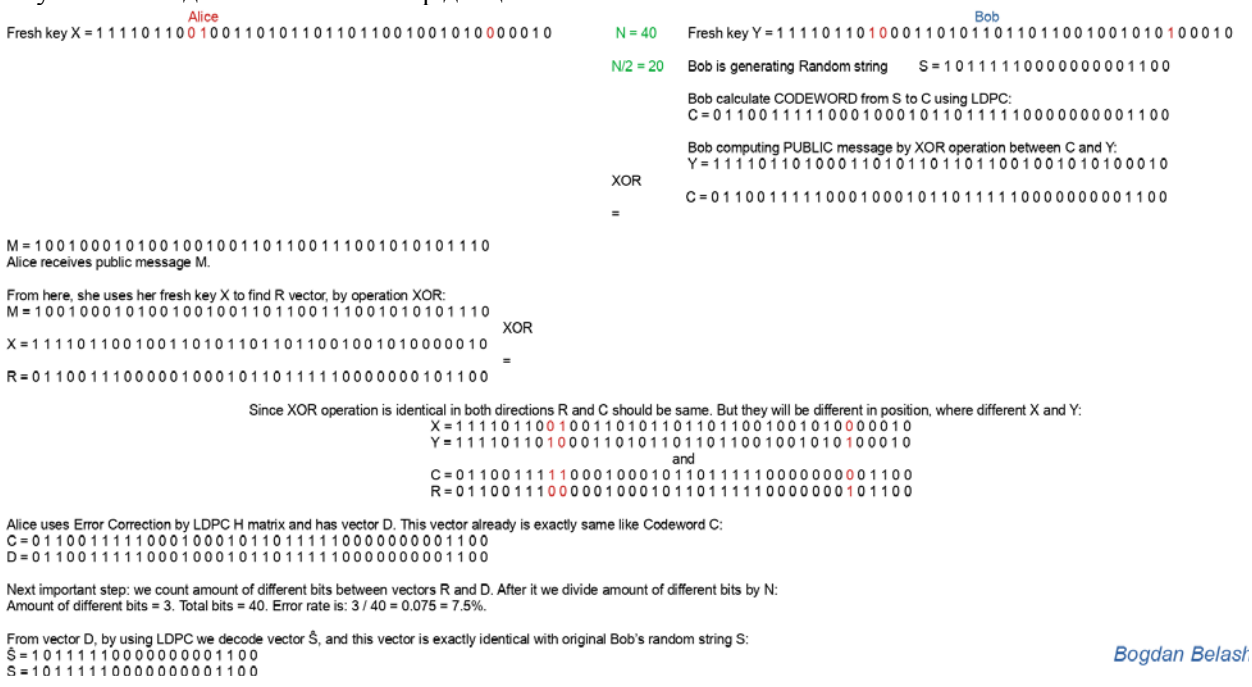
R = 0 1 1 0 0 1 1 1 0 0 0 0 0 1 0 0 0 1 0 1 1 0 1 1
1 1 1 0 0 0 0 0 0 0 1 0 1 1 0 0

7. Визначення вектору D. Після корекції помилок цей вектор співпадає з вектором C.




8. Обчислення вектору помилок (дорівнює 7,5%).

9. Отриманий вектор $\hat{S}$ дорівнює оригінальному вектору S у Боба. Обидва вектори передаються на наступний етап для посилення конфіденційності.



**Висновки**

Адаптовано відомий метод корекції помилок CV-QKD систем, у якому модулюється кодове слово з корельованою гаусовою послідовністю, для застосування в DV-QKD системах шляхом використання просіяного ключа у вигляді класичних бітів, з яких створюється кодове слово, а також шифру Вернама, у якому використовується достатньо проста в реалізації класична булева операція XOR.

В запропонованому рішенні квантова складова протоколу відбувається лише на першому етапі передачі захищеного ключа, де відбувається обмін фотонами. На відміну від CV-QKD систем, де ненадійний квантовий канал з високим впливом шумів застосовується на другому та третьому етапах, згідно запропонованому рішенню на цих етапах використовуються класичні біти, що транспортуються по класичному каналу, який з високим ступенем вірогідності вважається надійним.

На відміну від інших відомих систем QKD, де на етапі корекції помилок просіяні ключі виправляються та переходять на наступний етап посилення конфіденційності, в модифікованому методі запропоновано використовувати просіяні ключі як ключі в шифрах Вернама, а вектор, який буде йти на наступний етап, генерувати випадковим чином та поєднувати з просіяним ключем. Відмінність у просіяних ключах Аліси та Боба виправляється за допомогою LDPC матриць, які заздалегідь відомі Алісі та Бобу.

***ЛІТЕРАТУРА***

1. **Ekert A. K.**, “Quantum Cryptography and Bell’s Theorem,” P.P. 413–418, 1992, DOI: 10.1007/978-1-4615-3386-3_34.

2. **Rivest R. L.**, Shamir A., and Adleman L., “A method for obtaining digital signatures and public-key cryptosystems” *Commun. ACM*, vol. 21, № 2. Pp. 120–126, Feb. 1978, DOI: 10.1145/359340.359342.

3. **Bennett C. H.** and Brassard G., “BB84 highest.pdf,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Pp. 174–179, 1984.

4. **Sibson P.** *et al.*, “Chip-based quantum key distribution,” *Nat. Commun.*, vol. 8, May 2016, 2017, DOI: 10.1038/ncomms13984.

5. **Lucamarini M.**, Yuan Z. L., Dynes J. F., and Shields A. J., “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, № 7705. Pp. 400–403, May 2018, DOI: 10.1038/s41586-018-0066-6.

6. **Yuan Z.** *et al.*, “10-Mb/s Quantum Key Distribution,” *J. Light. Technol.*, vol. 36, № 16. Pp. 3427–3433, 2018, DOI: 10.1109/JLT.2018.2843136.

7. **Lo H.-K.**, Curty M., and Qi B., “Measurement-Device-Independent Quantum Key Distribution,” *Phys. Rev. Lett.*, vol. 108, №.13, P. 130503, Mar. 2012. DOI: 10.1103/PhysRevLett.108.130503.

8. **Park C. H.** *et al.*, “Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing,” *IEEE Access*, vol. 6. Pp. 58587–58593, 2018, DOI: 10.1109/ACCESS.2018.2874028.

9. **Park B. K.**,. Woo M. K, Kim Y.-S., Cho Y.-W., Moon S., and Han S.-W., “User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1 × N quantum key distribution network system,” *Photonics Res.*, vol. 8, № 3. P. 296, Mar. 2020, DOI: 10.1364/PRJ.377101.

10. **Eriksson T. A** *et al.*, “Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission,” *IEEE Photonics Technol. Lett.*, vol. 31, № 6. Pp. 467–470, 2019, DOI: 10.1109/LPT.2019.2898458.

11. **Brassard G.** and Salvail L., “Secret-key reconciliation by public discussion,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 765 LNCS. Pp. 410–423, 1994, DOI: 10.1007/3-540-48285-7_35.

12. **Buttler W. T.**, Lamoreaux S. K., Torger son J. R., Nickel G. H., Donahue C. H., and Peter son C. G., “Fast, efficient error reconciliation for quantum cryptography,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 67, № 5. P. 8, 2003, DOI: 10.1103/PhysRevA.67.052303.

13. **Gallager**, “Low density parity check codes,” 1963.

14. **Ma**ckay **D. J. C.** and Neal R. M., “Good codes based on very sparse matrices,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1995, vol. 1025. Pp. 100–111, DOI: 10.1007/3-540-60693-9_13.

15. **MacKay D. J. C.**, “Good error-correcting codes based on very sparse matrices,” *IEEE Trans. Inf. Theory*, vol. 45, № 2. Pp. 399–431, 1999, DOI: 10.1109/18.748992.

16. **Milicevic M.**, Feng C., Zhang L. M., and. Gulak P. G, “Key Reconciliation with Low-Density Parity-Check Codes for Long-Distance Quantum Cryptography,” № April. Pp. 1–23, 2017. DOI: 10.1038/s41534-018-0070-6.

17. **S. Vernam**, “Secret signaling system,” 1919.

18. **Shannon C. E.**, “Communication Theory of Secrecy Systems,” *Bell Syst. Tech. J.*, vol. 28, № 4. Pp. 656–715, 1949, DOI: 10.1002/j.1538-7305.1949.tb00928.x.

19. **Peng W.**, Cheng D., and Song C., “One-time-pad cryptography scheme based on a three-dimensional DNA self-assembly pyramid structure,” *PLoS One*, vol. 13. № 11. P. e0206612, Nov. 2018. DOI: 10.1371/journal.pone.0206612.

**Білаш Б. О.**

## МОДИФІКОВАНИЙ МЕТОД КОРЕКЦІЇ ПОМИЛОК ІЗ ЗАСТОСУВАННЯМ ШИФРУ ВЕРНАМА У СИСТЕМАХ QKD

*В даній роботі проаналізовано та адаптовано відомий метод корекції помилок CV-QKD систем, запропонований Маріо Міліцевичем, у якому модулюється кодове слово з корельованою гаусовою послідовністю в амплітудній та фазовій квадратурах когерентних станів, для застосування в DV-QKD системах, в який інформація кодується в поляризації однофотонних станів, шляхом використання просіяного ключа у вигляді класичних бітів, з яких створюється кодове слово, а також одноразового шифру Вернама, у якому використовується достатньо проста в реалізації класична булева операція «виключне або». Наразі розвиваються два напрямки підвищення надійності систем QKD: дослідження квантового каналу на фізичному рівні та корекція помилок після створення просіяного ключа. Основне завдання корекції помилок полягає у виправленні помилок, щоб поділитися однаковим захищеним ключем між двома сторонами (які, зазвичай звуться Алісою та Бобом). Причиною виникнення помилок можуть бути різні фактори. Ненадійність квантового каналу обумовлена тим, що фотони можуть викликати шум при зміні вектора поляризації фотона. В запропонованому рішенні квантова складова протоколу відбувається лише на першому етапі передачі захищеного ключа, де відбувається обмін фотонами. Система квантового розподілу ключів має неминучі помилки в просіяному ключі, які повинні бути виправлені алгоритмом виправлення помилок для створення захищеного ключа. На відміну від інших відомих QKD систем, де на етапі корекції помилок просіяні ключі виправляються та переходять на наступний етап посилення конфіденційності, в модифікованому методі запропоновано використовувати просіяні ключі як ключі в одноразових шифрах Вернама, а вектор, який буде йти на наступний етап, генерувати випадковим чином та поєднувати з просіяним ключем. Відмінність у просіяних ключах між двома сторонами виправляється за допомогою матриць перевірки на парність (LDPC), які заздалегідь відомі їм обом. Матриці перевірки на парність створюються алгоритмом, запропонованим Девідом Маккеєм та Редфордом Нілом.*

**Ключові слова:** QKD; LDPC; корекція помилок; parity-check matrix; post-processing

**Bilash B.**

## MODIFIED ERROR CORRECTION METHOD USING ONE-TIME PAD IN QKD SYSTEMS

*This paper analyzes and adapts the known method of error correction of CV-QKD systems, proposed by Mario Milicevic, which modulates a code word with a correlated Gaussian sequence in amplitude and phase quadratures of coherent states, for use in DV-QKD systems, in which information is encoded by single-photon polarization states, by using a sieved key in the form of classical bits, from which the codeword is created, and also a one-time pad (Vernam cipher), which uses a fairly easy to implement classic Boolean "exclusive OR" operation (XOR). The main task of error correction is to correct errors in order to share the same secure key between the two parties (usually called Alice and Bob). Various factors can cause errors. The unreliability of the quantum channel is due to the fact that photons can cause noise when changing the polarization vector of the photon. In the proposed solution, the quantum component of the protocol occurs only in the first stage of transmission of the protected key, where the exchange of photons. The quantum key distribution system has inevitable errors in the sieved key, which must be corrected by the error correction algorithm to create a secure key. Unlike other known QKD systems, where at the stage of error correction the sifted keys are corrected and passed to the next stage of increasing confidentiality, in the modified method it is proposed to use sifted keys as keys in disposable Vernam ciphers, and the vector that will go to the next stage way and combine with the sifted key. The difference in the sieved keys between the two parties is corrected by means of low-density parity check matrices (LDPC), which are known to both of them in advance. Parity check matrices are created by an algorithm proposed by David MacKay and Radford Neal. Radford Neal open-source program code, is used to create final work program to checking proposed algorithm.*

**Keywords**: QKD; LDPC; error correction; parity-check matrix; post-processing.

**Белаш Б. О.**

## МОДИФИЦИРОВАННЫЙ МЕТОД КОРРЕКЦИИ ОШИБОК С ИСПОЛЬЗОВАНИЕМ ШИФРА ВЕРНАМА В СИСТЕМАХ QKD

*В данной работе проанализирован и адаптирован известный метод коррекции ошибок CV-QKD систем, предложенный Марио Милицевичем, в котором модулируется кодовое слово с коррелированной гауссовой последовательностью в амплитудной и фазовой квадратурах когерентных состояний, для применения в DV-QKD системах, в которых информация кодируется в поляризации однофотонных состояний, путём использования просеянного ключа в виде классических битов, из которых создаётся кодовое слово, а также одноразового шифра Вернама, в котором используется достаточно простая в реализации классическая булева*

*операция «исключающее или». Сейчас развиваются два направления повышения надёжности систем QKD: исследования квантового канала на физическом уровне и коррекция ошибок после создания просеянного ключа. Основная задача коррекции ошибок заключается в исправлении ошибок для того, чтобы поделиться одинаковым защищённым ключом между двумя сторонами (которые, как правило, называют Алисой и Бобом). Причиной возникновения ошибок могут служить различные факторы. Ненадёжность квантового канала обусловлена тем, что фотоны могут вызвать шум при изменении вектора поляризации фотона. В предлагаемом решении квантовая составляющая протокола происходит на первом этапе передачи защищённого ключа, где происходит обмен фотонами. Система квантового распределения ключей имеет неизбежные ошибки в просеянном ключе, которые должны быть исправлены алгоритмом исправления ошибок для создания защищённого ключа. В отличие от других известных QKD систем, где на этапе коррекции ошибок просеянные ключи исправляются и переходят на следующий этап усиления конфиденциальности, в модифицированном методе предложено использовать просеянные ключи как ключи в одноразовых шифрах Вернама, а вектор, идущий на следующий этап, генерировать случайным образом и сочетать с просеянной ключом. Различие в просеянных ключах между двумя сторонами исправляется с помощью матриц проверки на чётность (LDPC), которые заранее известны обоим сторонам. Матрицы проверки чётности создаются методом, предложенным Дэвидом Маккеем и Редфордом Нилом.*

**Ключевые слова:** QKD; LDPC; коррекция ошибок; parity-check matrix; post-processing

Стаття надійшла до редакції 06.05.2020 р.
Прийнято до друку 18.06.2020 р.