DOI: 10.18372/2310-5461.51.15692
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

О. М. Лисенко, д-р техн. наук, проф.
Національний технічний університет України
"Київський політехнічний інститут ім. Ігоря Сікорського"
orcid.org/0000-0003-1051-1149
e-mail: o.m.lysenko@kpi.ua

УДОСКОНАЛЕНИЙ МЕТОД ВИПРАВЛЕННЯ ПОМИЛОК ІЗ ВИКОРИСТАННЯМ НА ЕТАПІ ПОСТ-ОБРОБКИ LDPC-КОДІВ У СИСТЕМАХ QKD

Вступ

Квантова криптографія на сьогодні є досить молодим, проте перспективним напрямком досліджень в науковому світі. Усі дослідження в квантовій криптографії базуються на законах квантової фізики, що є спільною ознакою для вже відомих методів квантової криптографії [1]. Однак наразі квантова криптографія є досить недостатньо детермінованою та класифікованою [2]. Тому існують декілька методів застосування квантової криптографіїї, над якими працюють дослідники всього світу. Одним із найбільш перспективних методів сучасної квантової криптографії [3] наразі є метод квантового розповсюдження ключів (Quantum Key Distribution, QKD), який виключає можливість злому квантовими алгоритмами [4] класичних криптографічних протоколів та дозволяє створити випадкові квантові ключі.

Постановка проблеми

Зазначений вище метод QKD є прикладом використання процедури шифрування із симетричним ключем. Однак, на відміну від протоколів, які генерують псевдовипадкові ключі, він надає можливість створення дійсно випадкових ключів завдяки використанню законів квантової фізики. Джерелом генерування таких ключів можуть бути як поляризація фотонів [5], так і їх представлення у вигляді кореляційної гауссівської послідовності [6]. Проте обидва ці підходи мають спільний недолік, обумовлений як наявністю перешкод у ненадійному квантовому каналі, так і можливими змінами квантового стану фотонів, викликаних третьою стороною, наслідком чого є зниження надійності системи.

Наразі провідні науковці всього світу працюють над усуненням зазначених вище проблем. При цьому можливими шляхами їх вирішення є:

- розробка нових алгоритмів QKD;
- підвищення надійності фізичних установок;
- розробка приладів, які генерують дійсно однофотонні порції сигналів;
- виправлення та корекція квантових помилок на основі класичних методів.

У цій статті увага буде сконцентрована саме на використанні останнього підходу.

Аналіз останніх досліджень і публікацій

За час свого існування квантова криптографія та методи і системи QKD набули широкого застосування у різних областях. Як приклад наукових досліджень за цією тематикою можна навести роботи по розробленню систем зменшення розмірів мікросхем [7], комунікацій на великі відстані [8], високої та безпечної швидкості передачі ключа QKD [9–11] тощо.

Квантова криптографія передбачає виконання двох основних етапів:

- етап QKD, на якому відбувається обмін фотонами по квантовому каналу; саме тут забезпечується дійсно випадкова послідовність кубітів, які потім перетворюються в класичні біти;

• етап пост-обробки, під час якого вже перетворені біти складаються в просіяний ключ; окремі його біти можуть бути помилковими, тому потребують виправлення класичними методами.

Такий розподіл квантової криптографії на етапи було запропоновано ще в першому квантовому протоколі BB84 [3]. Ця концепція застосовується і досі. Не зважаючи на те, що домінантою другого етапу пост-обробки є, насамперед, використання математичного апарату, на ньому також досягнуто немалих успіхів, зокрема, при розробленні ефективних алгоритмів корекції помилок [12; 13].

Процедура пост-обробки базується на виявленні частоти квантових помилок по бітам (*quantum bit error rate*, QBER). Її основним завданням є виправлення виявлених помилок згідно QBER між двома сторонами, які, зазвичай, звуться Алісою та Бобом. Залежно від значення QBER, а також довжини повідомлення і відстані між сторонами, можуть застосовуватись різні методи виправлення помилок, про які мова йтиме нижче. За замовчуванням, помилки виникають на етапі зчитування стану фотонів Бобом через те, що детектор фотонів є надзвичайно чутливою складовою для їх виявлення.

На цей детектор найбільш вагомий вплив спричиняє шум в оптичному каналі під назвою Cross talk [14]. Авторами протоколу BB84 емпіричним шляхом було встановлено, що при реалізації їх протоколу QBER має не перевищувати 11 %. Якщо це так, QBER обумовлено впливом саме шумів під час обміну фотонами на усьому етапі QKD. Якщо QBER складає більше 11 %, значить присутні аномалії, викликані впливом третьої сторони (підслуховувача, *eavesdropper*, якого, зазвичай, звуть Євою).

Останні успіхи в розробці приладів для генерування та зчитування фотонів дозволяють отримувати QBER не більше 5 %. Проте досі залишаються проблемними так звані лавинні порції фотонів, які зчитуються як один стан фотону. Однак, на етапі пост-обробки основним є виправлення помилок із врахуванням шумів, які виникли саме під час фази обміну фотонами і є вже наявними постфактум.

Мета

Дослідження методів виправлення помилок в системах квантової криптографії на етапі пост-обробки (корекції помилок) для створення справді випадкових ключів, які можна використовувати, наприклад, у шифрах Вернама, що мають властивість абсолютної криптографічної стійкості.

1. Огляд існуючих методів виправлення помилок

Протягом останніх 35 років науковцями запропоновано низку методів виправлення квантових бітових помилок, деякі з яких створені з нуля, деякі — адаптовані з класичних методів до квантової криптографії. Частково їх аналіз вже було здійснено одним із авторів в роботі [13]. Тому зупинимось коротко на найбільш популярних із них.

Авторами протоколу BB84 у праці [15] було запропоновано метод Cascade, згідно якому в кожному проході Аліса та Боб домовляються про випадкову перестановку їхніх бітів. Комбінацією цього методу та відомих кодів Хеммінга з'явився метод Winnow [16]. При його реалізації, як і методу Cascade, здійснюється поділ двійкових рядків на блоки, але замість виправлення помилок за допомогою ітеративної бінарної фіксації застосовуються синдроми, які базуються на матриці перевірки на парність кодів Хеммінга. Однак, як зазначалось вище, окрім QBER на ефективність методів корекції помилок впливають також довжина повідомлень Аліси та Боба, а також відстань між ними. На жаль, для цих параметрів обидва зазначені вище методи показали свою неефективність. Цьому не сприяла також реалізація в обох методах ітеративних процедур, які потребують для виконання занадто багато часу.

Тому виникла потреба у створенні такого підходу, який би дозволив розмістити контрольні біти разом з основним повідомленням за один раз під час транспортування. Виявилось, що це може бути досягнуто шляхом використання LDPC-кодів (l*ow density parity check*, LDPC) [17], які застосовуються в класичних телекомунікаційних системах, є досить ефективними у виправлені помилок [15–19] та можуть бути адаптовані для квантової криптографії. Про те, яким чином здійснювалась ця адаптація для систем QKD, детально викладено в роботі [19]. Слід також згадати і про відомих фахівців Д. Маккея та Р. Ніла, які внесли свій суттєвий вклад у розвиток класичного методу LDPC [18; 19].

2. Квазіциклічні LDPC-коди

Запропонований Д. Маккеєм та Р. Нілом метод LDPC має високу ефективність для невеликих по довжині повідомлень, а, отже, і невеликих розмірах матриць перевірки. При його реалізації здійснюється випадкова генерація матриць перевірки з випадковим розміщенням ненульових елементів у стовпцях та рядках. Проте, коли довжина повідомлень є великою, дуже складно генерувати такі матриці перевірки з випадковим розміщенням елементів.

Як альтернативу в праці [21] було запропоновано використання квазіциклічних LDPC-кодів (*quasicyclic* LDPC *codes*, QC-LDPC). Основною ідеєю тут є застосування так званих матриць-циркулянтів (*circulant matrix*), у яких елементи кожного наступного рядка зсунуті циклічно вправо на один елемент (рис. 1).

$$C = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

Рис. 1. Загальний вигляд матриці-циркулянта

Такий спосіб побудови матриці перевірки має такі переваги:

– відпадає необхідність генерувати випадковим чином ненульові елементи в матриці;
– виключається можливість виникнення циклів;
– значно простіша апаратна реалізація.

Детальніше про створення QC-LDPC-кодів викладено в роботі [22].

Як видно із рис. 1, згенерувавши лише перший рядок можна створити всю матрицю перевірки. Зупинимось на розгляді вже кінцевого варіанту матриці, яку було створено авторами (рис. 2).

$$H = \left[\begin{array}{cccc|cccc} 1 & 1 & & & 1 & & 1 & 1 \\ & 1 & 1 & & 1 & 1 & & 1 \\ & & 1 & 1 & & 1 & 1 & & 1 \\ & & & 1 & 1 & 1 & & 1 & \\ 1 & & & & & 1 & & 1 & 1 \end{array}\right]$$

Рис. 2. Створена матриця перевірки

Наведена вище матриця перевірки складається із двох двійкових матриць-циркулянтів. Згідно з працею [20] цієй матриці перевірки відповідає породжувальна матриця, яка в свою чергу складається з одиничної матриці та матриці перевірки на парність (рис. 3).

$$G = \left[\begin{array}{ccccc|cccc} 1 & & & & & 1 & & 1 & \\ & 1 & & & & & 1 & & 1 \\ & & 1 & & & 1 & & 1 & \\ & & & 1 & & & 1 & & 1 \\ & & & & 1 & & & 1 & 1 \end{array}\right]$$

Рис. 3. Породжувальна матриця

Алгоритм кодування та декодування даних із застосування матриць-циркулянтів є типовим для LDPC-кодів та відповідає запропонованому Р. Галагером у праці [17].

3. Кільце поліномів над полями Галуа

Використання матриць-циркулянтів для QC-LDPC систем призвело до значного підвищення ефективності кодування та уникнення циклів. Проте, за значних розмірів повідомлень збільшуються і розміри матриці, яка потребує більше пам'яті в апаратних ресурсах. Це досі залишається однією з головних проблем застосування LDPC-кодів.

Для вирішення цієї проблеми пропонується використати поліноми над полями Галуа.

Згідно з працею [23] будь-яка матриця-циркулянт є ізоморфною, тобто може бути описана певним поліномом в кільці поліномів над полями Галуа [24]. Тобто матриця H (рис. 2) складається з двох матриць-циркулянтів, які можуть бути описані комбінацією бітів першого рядка: A_1 = 11000; A_2 = 10101. Відповідним поліномом для циркулянта A_1 є $a_1(x) = x^4 + x^3$; для циркулянта A_2 – $a_1(x) = x^4 + x^2 + 1$.

Проте в апаратних ресурсах дані зберігаються у вигляді послідовності бітів.

Використання таких ізоморфних властивостей поліномів дає змогу значно простіше створювати та зберігати не лише матрицю перевірки, а і породжувальну матрицю. Для цього достатньо використовувати властивості кілець поліномів над полями Галуа [24]. Для знаходження зворотного полінома використовується метод Евкліда-Уолліса [25].

Адаптований алгоритм знаходження зворотного полінома для реалізації за допомогою програмного забезпечення запропоновано на рис. 4 (в алгоритмі поняття «поліном» означає послідовність бітів).

У результаті породжувальна матриця буде представлена у вигляді полінома або масиву даних, який являє собою лише перший рядок матриці-циркулянта. При швидкостях коду [26] більше ніж ½ розмір породжувальної матриці експоненційно збільшується у порівнянні з розміром матриці перевірки. Отже, обидві матриці можна представити лише їх першими рядками.

Програмне забезпечення, яке реалізує наведений вище алгоритм, розглянуто в праці [27].

4. Адаптований алгоритм розповсюдження довіри для декодування повідомлень

Р. Галагер в своїй праці [17] запропонував для декодування повідомлень два алгоритми, розглянуті ним в теоретичному вигляді: жорсткий (bit-flipping) та м'який (розповсюдження довіри або sum-product algorithm, SPA).

Жорсткий алгоритм показав низьку ефективність, тому практичного використання отримав лише м'який, що зумовило його використання в цій роботі.

Algorithm 1 Алгоритм створення зворотнього полінома

Вхідні дані: Вхідний поліном, незвідний поліном

```
Позначаємо незвідний поліном як ділене, вхідний поліном як дільник
while True do
    Тимчасовий дільник ← дільник
    while True do
        Вираховуємо різницю ступенів поліномів між діленим і дільником
        Зсуваємо дільник право на кількість, рівну різниці ступенів поліномів між діленим і дільником
        Робимо логічну операцію XOR між діленим і дільником та зберігаємо в новий масив результату
        У массиві коефіцієнтів зсуву встановлюємо одиницю в позиції, номер якої відповідає разниці ступенів поліномів між діленим і дільником
        Присвоюємо новому масиву, який є тимчасовим діленим значення дільника
        if Старший біт тимчасового діленого більше дільника then
            break
        else Перевірка розрядності дільника і діленого
        end if
    end while
    Ділене ← Дільник
    Дільник ← Результат
    if Ділене = 0 then
        break
    end if
end while
```

Рис. 4. Алгоритм створення зворотного полінома

Як зазначено у роботі [22], матриця перевірки та породжувальна матриця, які використовуються в алгоритмі SPA, можуть бути представлені у вигляді поліномів. Похідні матриці утворюються окремо з матриць перевірки.

В цій роботі запропоновано адаптований алгоритм SPA на основі поліномів для створення похідних матриць, який декодує та виправляє помилки. Цей алгоритм наведено на рис. 5.

Створене власне програмне забезпечення, яке реалізує наведений вище алгоритм, наведено у праці [27]. Підтверджено працездатність адаптованого алгоритму SPA, який дозволяє підвищити ефективність декодування та виправлення помилок у порівнянні з базовим м'яким алгоритмом, запропонованим Р. Галагером, за рахунок скорочення часу обчислення поліномів у порівнянні з часом обчислення матриць.

Приклад роботи програмного забезпеення для поліномів довжиною і 5 бітів наведено на рис. 6.

Algorithm 2 Адаптований алгоритм SPA

Вхідні дані: Матриця перевірки, прийнятий вектор повідомлення

Створення синдрому шляхом матричного перемноженя матриці перевірки та прийнятого вектора повідомлення
if Синдром = 0 then
    Прийнятий вектор є кодовим словом. Кінец алгоритму.
else
    створення коефіцієнту згідно з коефіцієнтом помилок
    Підготовка початкових коефіцієнтів для нулів і одиниць
    масиву з коефіцієнтами логарифмічного відношення
    створення M матриці та заповнення її
    while True do
        Створення E матриці згідно M матриці та асиву з коефіцієнтами логарифмічного відношення
        створення нового L вектору з м'якими коефіцієнтами
        створення на основі L вектору нового вектора, який є кандидатом на кодове слово
        Створення синдрому шляхом матричного перемноженя матриці перевірки та вектору-кандидата на кодове слово
        if Синдром = 0 then
            Прийнятий вектор є кодовим словом. Кінец алгоритму.
            break
        end if
    end while
end if

Рис. 5. Адаптований алгоритм SPA декодування та виправлення помилок

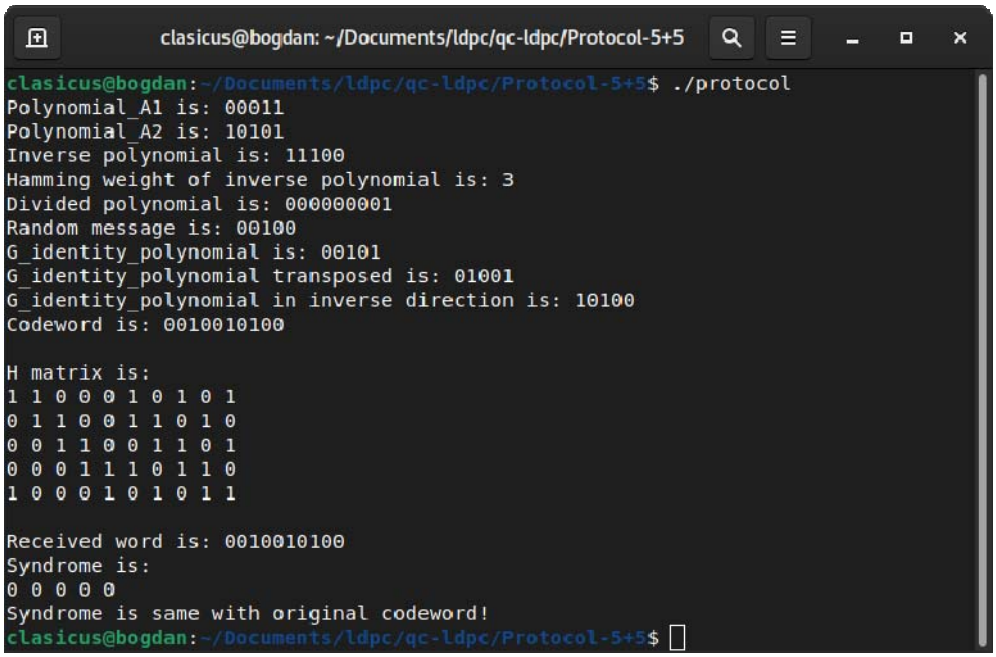

Рис. 6. Приклад роботи програмного забезпечення для поліномів довжиною і 5 бітів

Висновки

З метою корекції квантових помилок в системах QKD запропоновано використання квазициклічних QC-LDPC матриць перевірки, які мають в своїй основі матриці-циркулянти. Такий спосіб побудови матриці перевірки дає такі переваги:

- відпадає необхідність генерувати випадковим чином ненульові елементи в матриці;
- виключається можливість виникнення циклів;
- значно простіша апаратна реалізація.

Удосконалено метод виправлення квантових помилок в системах QKD з використанням QC-LDPC-кодів шляхом врахування властивості ізоморфності матриць-циркулянтів і кілець поліномів над полями Галуа та використання поліномів замість матриць, що дозволило зменшити апаратні ресурси для їх зберігання та підвищити швидкодію методу.

Реалізація удосконаленого методу досягається через:

– розроблення адаптованого алгоритму знаходження породжувальної матриці у вигляді ізоморфного до неї поліному, який базується на використанні в теоретичному вигляді методу Евкліда-Уолліса та створення програмного забезпечення для впровадження цього алгоритму;

– адаптації м'якого алгоритму SPA, запропонованого в теоретичному вигляді Р. Галагером, для виконання декодування і виправлення помилок та створення програмного забезпечення виконання цього алгоритму.

ЛІТЕРАТУРА

[1] Gnatyuk, S., Okhrimenko, T., Azarenko, O., Fesenko, A., Berdibayev, R. (2020). Experimental Study of Secure PRNG for Q-trits Quantum Cryptography Protocols. *Procedings of 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (May 14–18, 2020, Kyiv).

[2] Gnatyuk, S. (2013). COMPARATIVE ANALYSIS OF QUANTUM KEY DISTRIBUTION SYSTEMS. *Naukoiemni Tekhnologiii.* Vol. 17 No. 1 (2013). https://doi.org/10.18372/2310-5461.17.4761

[3] Ekert, A. (1992). Quantum Cryptography and Bell's Theorem. *Physical Review Letters.* P. 413–418. (1992) https://doi.org/10.1103/ PhysRevLett.67.661

[4] Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput*. Soc. Press: 124–134. (1994). https://doi.org/10.1109/sfcs.1994.365700

[5] Bennett, C., Brassard, G. (1984) BB84, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Pp. 174–179. (1984).

[6] M. Milicevic, M., Feng, C., Zhang, L., Gulak, P. (2017). Key Reconciliation with Low-Density Parity-Check Codes for Long-Distance Quantum Cryptography. Pp. 1–23. (2017). https://doi.org/10.1038/s41534-018-0070-6

[7] Sibson, P. (2016). Chip-based quantum key distribution. *Nat. Commun.* (Vol. 8, May, 2016). https://doi.org/10.1038/ncomms13984

[8] Lucamarini, M., Yuan, Z., Dynes, J., Shields A. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature.* Vol. 557, №.7705, P.P. 400–403 (May, 2018). https://doi.org/ 10.1038/s41586-018-0066-6

[9] Yuan, Z. (2018). 10-Mb/s Quantum Key Distribution. *J. Light. Technol.* Vol. 36, p. 3427–3433. (2018). https://doi.org/10.1109/ JLT.2018.2843136.

[10] Lo, H., Curty, M., Qi, B. (2012). Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* Vol. 108, №.13, p. 130503. (Mar. 2012). https://doi.org/ 10.1103/PhysRevLett. 108.130503.

[11] Park, C. (2018). Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing. *IEEE Access.* Vol. 6, p. 58587–58593. (2018). https://doi.org/10.1109/ ACCESS. 2018.2874028.

[12] Park, B., Woo, M., Kim, Y., Cho, Y., Moon, S., Han, S. (2020). 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). https://doi.org/10.1364/PRJ.377101.

[13] Bilash, B. (2020). Modified Error-Correction method based on one-time pad in quantum key distribution systems. *Naukoiemni Tekhnologiii* №2 (46), C. 129-136 (2020) https://doi.org/ 10.18372/2310-5461.46.14803 (In Ukrainian).

[14] Eriksson, T. (2019). Crosstalk Impact on Continuous Variable Quantum Key Distribution in Multicore Fiber Transmission. *IEEE Photonics Technol. Lett.*, Vol. 31, №.6, p. 467–470. (2019). https://doi.org/10.1109/ LPT.2019.2898458

[15] Brassard, G., Salvail, L. (1994). Secret-key reconciliation by public discussion. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. Vol. 765 LNCS, p. 410–423. (1994) https://doi.org/10.1007/3-540-48285-7_35

[16] Buttler, W., Lamoreaux, S., Torgerson, J., Nickel, G., Donahue, C., Peterson, C. (2003). Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A – At. Mol. Opt. Phys.*, vol. 67, №.5, p. 8. (2003) https://doi.org/10.1103/PhysRevA.67.052303

[17] Gallager, R. (1963). Low density parity check codes. *Cambridge: M.I.T. Press*. P. 90. (1963).

[18] Mackay D., Neal, R. (1995). Good codes based on very sparse matrices. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Vol. 1025, p. 100–111. https://doi.org/10.1007/3-540-60693-9_13

[19] MacKay, D. (1999) Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inf. Theory.* Vol. 45, №.2, p. 399–431. (1999). https://doi.org/10.1109/18.748992

[20] Bilash, B., Park, B., Park, C., Han, S. (2020). Error-Correction Method Based on LDPC for Quantum Key Distribution Systems. *2020 International Conference on Information and Communication Technology Convergence (ICTC).* https://doi.org/10.1109/ICTC49870.2020.9289451.

[21] Fossorier, M. (2004). Quasicyclic low-density parity-check codes from circulant permutation matrices. *Information Theory, IEEE Transactions.* Vol. 50, no. 8, p. 1788–1793. (Aug. 2004).

[22] Johnson, S. (2005). Introducing Low-Density Parity-Check Codes.

[23] Philip, D., Circulant Matrices, Wiley. *ISBN.* (New York, 1970).

[24] Vlasov, E. Finite fields in telecomuting applications. Theory and practice. *FEC, CRC.* Moscow: Nauka (In Russian).

[25] Linear diophanite equation. Retrieved from https://math.stackexchange.com/questions/67969/linear-diophantine-equation-100x-23y-19/68021#68021.

[26] Sibson, P. (2017). Chip-based quantum key distribution. *Nat. Commun.* Vol. 8, No. (May, 2016) https://doi.org/10.1038/ncomms13984.

[27] Inverse polynomial. Retrieved from https://notabug.org/clasicus/Studying/src/master/Quantum%20Cryptography/Error%20Correction/Inverse%20Polynomial

Білаш Б. О., Лисенко О. М.

УДОСКОНАЛЕНИЙ МЕТОД ВИПРАВЛЕННЯ ПОМИЛОК ІЗ ВИКОРИСТАННЯМ НА ЕТАПІ ПОСТ-ОБРОБКИ LDPC-КОДІВ У СИСТЕМАХ QKD

У статті проведено огляд відомих методів корекції помилок для систем QKD, визначено їх переваги та недоліки. Обґрунтовано для удосконалення метод LDPC-кодів. При обміні кубітів між Алісою та Бобом по квантовому каналу можуть виникати помилки через шуми, а також Боб під час вимірювання станів може отримувати помилкові значення, які необхідно виправляти на етапі пост-обробки. Матриця перевірки для LDPC-кодів є квазіциклічною, тобто кожний наступний рядок матриці є циклічно зсунутим вправо на один біт відносно попереднього рядка. Це дозволяє не лише описати матрицю лише першим рядком матриці, але і використати властивість ізоморфності матриць-циркулянтів з кільцем поліномів над полем Галуа. Тобто матриця перевірки може бути описана певним поліномом. І операції, які виконуються над цим поліномом, застосовуються і на матрицю. Використання таких ізоморфних властивостей поліномів дає змогу значно простіше створювати та зберігати не лише матрицю перевірки, а і породжувальну матрицю, що дозволяє уникнути довготривалих матричних перемножень та застосування більшої кількості пам'яті для зберігання даних матриці, в результаті значно спрощує апаратну реалізацію. Створення кодового слова відбувається методом, запропонованим автором LDPC-кодів Р. Галагером. Для декодування кодових слів у вихідне повідомлення застосовується «м'який» алгоритм розповсюдження довіри (belief-propagation algorithm) або sum-product algorithm (SPA), який показав свою ефективність та використовується в сучасних телекомунікаційних системах. Запропоновано та адаптовано для написання програмного коду алгоритм для генерування матриці перевірки та алгоритм для створення породжувальної матриці, який базується на методі для знаходження зворотного полінома Евкліда-Уолліса. Створено програмне забезпечення, яке реалізує вищесказані алгоритми, з яким можна ознайомитись на git-репозиторії.

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

Bilash B., Lysenko O.

ADVANCED ERROR CORRECTION METHOD USING LDPC CODES IN POST-PROCESSING STAGE IN QKD SYSTEMS

This paper reviews the known error correction methods for QKD systems, identifies their advantages and disadvantages. The method of LDPC-codes is substantiated for improvement. Noise errors can occur when exchanging qubits between Alice and Bob through the quantum channel, and Bob may receive erroneous values when measuring states that need to be corrected in the post-processing phase. The verification matrix for LDPC codes is quasi-cyclic, ie each subsequent row of the matrix is cyclically shifted to the right by one bit relative to the previous row. This allows

not only to describe the matrix only by the first line of the matrix, but also to use the property of isomorphism of circulating matrices with a ring of polynomials over the Galois field. That is, the verification matrix can be described by a certain polynomial. And the operations performed on this polynomial are applied to the matrix. Using such isomorphic properties of polynomials makes it much easier to create and store not only a test matrix but also a generating matrix, which avoids long-term matrix multiplications and the use of more memory to store matrix data, greatly simplifying hardware implementation. The code word is created by the method proposed by the author of LDPC-codes R. Gallagher. The decoding of code words in the original message uses a "soft" algorithm for spreading trust (belief-propagation algorithm) or sum-product algorithm (SPA), which has proven its effectiveness and is used in modern telecommunications systems. An algorithm for generating a verification matrix and an algorithm for generating a generating matrix based on the method for finding the inverse Euclidean-Wallis polynomial have been proposed and adapted for writing program code. Software has been created that implements the above algorithms, which can be found on the git repository.

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

Стаття надійшла до редакції 27.08.2021 р.
Прийнято до друку 11.10.2021 р.