УДК 003.26:621.39+530.145

Є.В. Василіу, кандидат фізико-математичних наук, доцент
(Одеська національна академія зв'язку ім. О.С. Попова, Україна)

СИНТЕЗ СТРУКТУРИ КВАНТОВОЇ СИСТЕМИ ПРЯМОГО БЕЗПЕЧНОГО ЗВ'ЯЗКУ

В роботі запропоновано загальний підхід до проблеми синтезу структури квантової системи прямого безпечного зв'язку. Детально описані схеми етапів такого синтезу для систем, що ґрунтуються на різних варіантах пінг-понг протоколу. Наведено результати застосування цього підходу до синтезу конкретних систем. Запропоновано стек протоколів, що реалізують безпечну квантову систему прямого передавання повідомлень.

Методи квантової криптографії швидко розвиваються протягом останніх двох десятиріч. На основі цих методів пропонуються нові підходи до побудови захищених систем конфіденційного зв'язку. Робота таких систем, які ґрунтуються на протоколах квантової криптографії, потребує використання не тільки самих цих протоколів, а і додаткових засобів класичної криптографії та кодування інформації для забезпечення високого рівня ефективності всієї системи та її стійкості як до атак зловмисника, так і до природних завад у квантових каналах зв'язку. Так, передавання інформації квантовим каналом є тільки одним з елементів стека протоколів квантового розподілення секретних ключів, інші елементи стека – це процедури виправлення помилок та підсилення секретності, які ґрунтуються на методах як квантової, так і класичної теорії інформації [1]. Відзначимо, що стійкість гібридної системи конфіденційного зв'язку, яка складається з квантової підсистеми розподілення секретних ключів та звичайної системи симетричного шифрування (наприклад, AES), визначається стійкістю останньої, оскільки сучасні квантові протоколи розподілення ключів забезпечують теоретико-інформаційній рівень стійкості при розподіленні ключів. Так, використання шифру Вернама в поєднанні з квантової системою розподілення ключів дозволить забезпечити теоретико-інформаційній рівень стійкості всієї системи конфіденційного зв'язку [2].

Існує інший підхід до побудови систем конфіденційного зв'язку з високим рівнем стійкості, який використовує інший напрямок квантових технологій захисту інформації – квантові протоколи прямого безпечного зв'язку. В таких протоколах повідомлення передається напряму, тобто без попереднього шифрування, що взагалі усуває складну проблему генерування, розподілення та зберігання секретних ключів. Але, системи конфіденційного зв'язку, які ґрунтуються на квантових протоколах прямого безпечного зв'язку, як правило, не можуть бути побудовані тільки на цих протоколах, а потребують додаткових засобів підсилення секретності, завадостійкого кодування тощо [3]. Тому постає проблема синтезу всіх цих елементів в єдину систему безпечного зв'язку, для чого потрібно розв'язати цілий ряд окремих завдань.

Так, першим етапом такого синтезу є розробка нового квантового протоколу (або вдосконалення за якимись параметрами вже запропонованого), тобто розробка схеми квантового кодування інформації та схеми контролю перехоплення інформації в квантовому каналі. Далі необхідно обчислити рівень стійкість протоколу до можливих видів атак, зокрема, атаки пасивного перехоплення, тобто обчислити кількість інформації, яка може бути перехоплена зловмисником у залежності від параметрів протоколу. Наступний етап синтезу, що ґрунтується на отриманих результатах аналізу стійкості протоколу, – це розробка процедур підсилення стійкості. Також необхідно вибрати ефективний завадостійкій код, квантовий або класичний, з урахуванням особливостей передавання інформації в даному протоколі. На рис. 1 показана схема цих етапів.

На даний час запропоновані різні види квантових протоколів прямого безпечного зв'язку. Більшість з них потребує передачі кубітів блоками. Це дозволяє виявити прослуховування квантового каналу до початку передавання самого повідомлення й таким способом гарантувати безпеку передачі – якщо прослуховування виявлене до передавання повідомлення, то легітимні користувачі переривають сеанс і ніяка інформація не попадає до зловмисника. Але

для зберігання таких блоків кубітів необхідна квантова пам'ять великого об’єму. Технологія квантової пам'яті активно розробляється, але ця технологія поки ще далека від масового застосування в стандартному телекомунікаційному встаткуванні. Тому з погляду технічної реалізації перевагу мають протоколи, у яких передавання здійснюється одиночними кубітами або невеликими їх групами (за один цикл протоколу). Одним з таких протоколів є так званий пінг-понг протокол [4], який не потребує для своєї практичної реалізації великої квантової пам'яті і може виконуватися з використанням існуючого технічного обладнання [5].

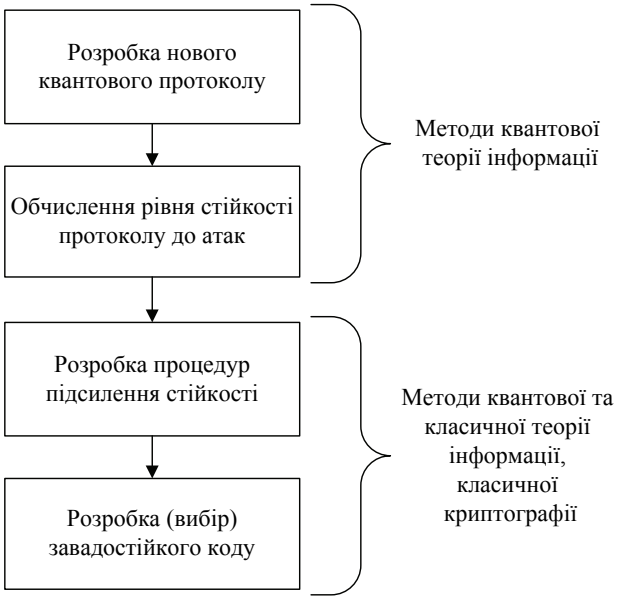

Рис. 1. Етапи синтезу структури квантової системи прямого безпечного зв’язку

В роботах автора розроблені декілька нових варіантів пінг-понг протоколу з використанням груп дво- та тривимірних квантових систем (кубітів та кутритів), які знаходяться в повністю переплутаних станах різного типу [6–8]. Використання багатокубітних або багатокутритних станів дозволяє значно збільшити інформаційну місткість пінг-понг протоколу. Таким чином, виконано перший етап синтезу структури квантової системи прямого безпечного зв’язку для різних варіантів базового протоколу. Також проаналізовано атаку пасивного перехоплення [3,9,10] та ряд інших атак [9] на розроблені варіанти пінг-понг протоколу, що є реалізацію другого етапу. На рис. 2 у логарифмічному масштабі наведені залежності повної ймовірності s невиявлення атаки пасивного перехоплення від кількості інформації I, що витікає до зловмисника, при деяких параметрах протоколів, які відповідають передаванню повідомлень з максимальною ентропією джерела, а також атаці, при який зловмисник прагне отримати як можна більше інформації.

Як видно з рис. 2, всі варіанти пінг-понг протоколу мають *асимптотичну* стійкість до атаки пасивного перехоплення, тобто атака буде виявлена, але зловмисник зможе перехопити деяку (невелику) кількість інформації. Щоб зробити інформацію, яка витекла до зловмисника, некорисною для нього, розроблено спеціальний спосіб підсилення стійкості пінг-понг протоколу [11]. Цей спосіб є оборотним гешуванням (гешуванням з використанням двосторонньої геш-функції) блоків відкритого тексту. Роль такої геш-функції грає випадкова, оборотна над полем Галуа GF(2) (або GF(3) для протоколу з кутритами) матриця чисел. При цьому розмір блоку відкритого тексту для гешування вибирається з умови, щоб ймовірність s невиявлення атаки пасивного перехоплення дорівнювала наперед заданої величині. Таким чином, синтезується квантова система прямого безпечного зв’язку з заданим рівнем стійкості до атаки пасивного перехоплення.

Також виконані оцінки обчислювальної складності генерації випадкових оборотних двійкових (розміру до 1000×1000) та трійкових (розміру до 200×200) матриць, та показано,

що час генерації таких матриць прийнятний навіть при використанні обчислювальної техніки з невисокою швидкодією [11]. Таким чином, виконано третій етап синтезу структури квантової системи прямого безпечного зв’язку, яка ґрунтується на пінг-понг протоколі.

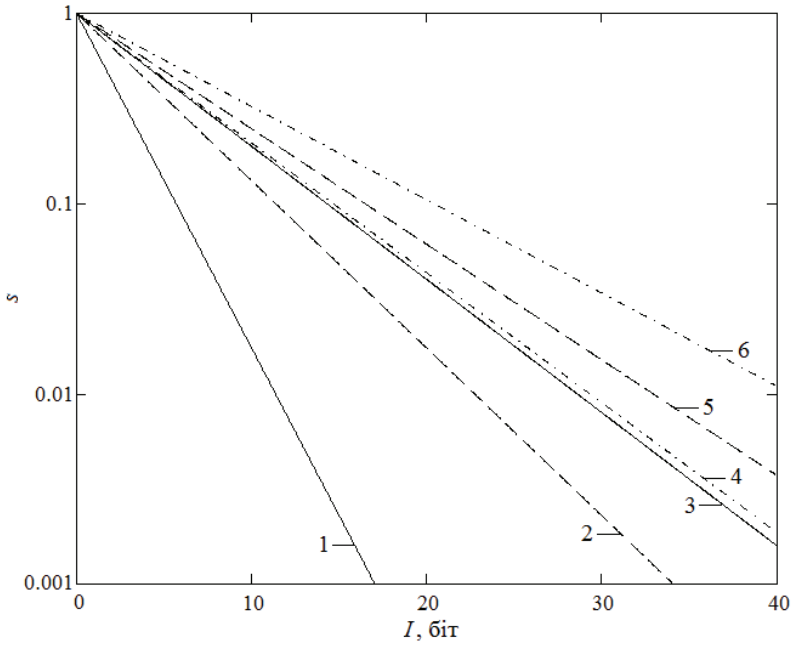

Рис. 2. Повна ймовірність *s* невиявлення атаки: 1 – оригінальний протокол; 2 – протокол з парами кубітів; 3 – протокол з парами кутритів; 4 – протокол з ГХЦ-четвірками кубітів; 5 – протокол з чотири-кубітними кластерними станами; 6 – протокол з ГХЦ-шестірками кубітів.

Четвертий етап синтезу пов'язаний з тим, що практичне використання квантової системи прямого безпечного зв’язку буде відбуватися не в ідеальних квантових каналах, а в реальних каналах з завадами. Оскільки квантові комунікаційні протоколи призначені для безпечного передавання *класичної* інформації квантовими каналами зв’язку, то для таких протоколів вигідніше використовувати *класичні завадостійкі коди*. Квантові завадостійкі коди, які розроблені на даний час [1], мають значно більшу надлишковість у порівнянні з відомими класичними. Для пінг-понг протоколу з парами Бела або ГХЦ-триплетами кубітів запропоновано використовувати код Файра, який виправляє пакети помилок довжиною до трьох бітів. Для протоколу з парами переплутаних кутритів запропоновано використовувати коди Ріда-Соломона над полем Галуа $GF(3^2)$. В роботі [12] побудовані таки коди та виконано оцінку їх корегувальної здатності. Отримана статистична інформація показує, що трійкові коди Ріда-Соломона добре справляються з корекцією помилок, якщо ймовірність деполяризації кутриту в квантовому каналі не перевищує 25-30% (в сучасних експериментах рівень помилок при передаванні фотонів квантовим каналом, як правило, не перевищує декількох процентів).

На рис. 3 показана послідовність (стек) протоколів, що реалізують режим передавання повідомлень для безпечної квантової системи зв’язку.

Висновки. В роботі запропоновано загальний підхід до проблеми структурного синтезу квантової системи прямого безпечного зв’язку й наведено результати застосування цього підходу до синтезу конкретних систем, які ґрунтуються на різних варіантах пінг-понг протоколу. Показано, що синтез складається з чотирьох етапів: розробка квантового протоколу прямого безпечного зв’язку; аналіз його стійкості до атак, зокрема атаки пасивного перехоплення; розробка процедур підсилення стійкості, які дозволять синтезувати систему з заданим рівнем стійкості; розробка (або вибір серед існуючих) класичного завадостійкого коду, який враховує особливості передавання інформації в даному квантовому протоколі. Розроблено стек протоколів, що реалізують режим передавання повідомлень для безпечної квантової системи зв’язку, яка використовує будь-який з варіантів пінг-понг протоколу в якості базового.

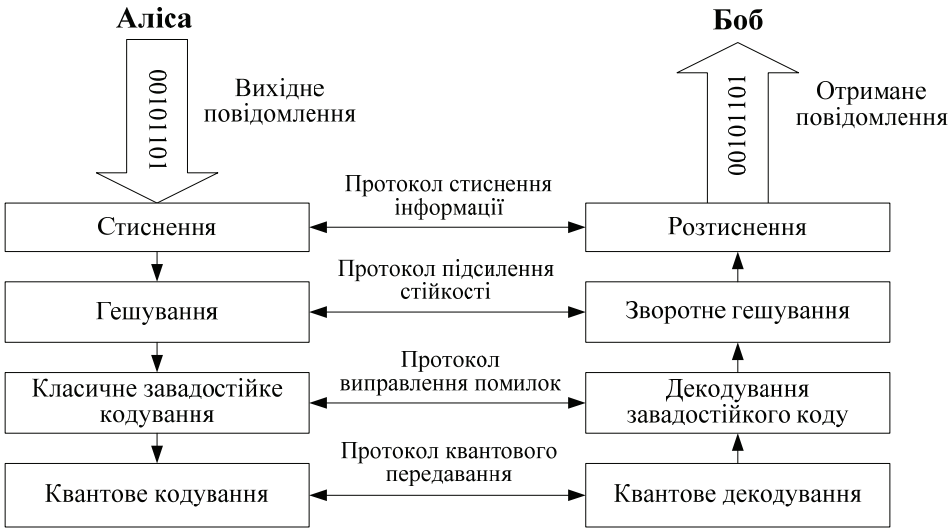

Рис. 3. Стек протоколів квантового прямого безпечного зв'язку

Список літератури

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

2. SECOQC White Paper on Quantum Key Distribution and Cryptography. – Preprint: http://www.arxiv.org/abs/quant-ph/0701168v1. – 2007. – 28 p.

3. Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83–91.

4. Bostrom K. Deterministic secure direct communication using entanglement / K. Bostrom, T. Felbinger // Physical Review Letters. – 2002. – V. 89, issue 18. – 187902.

5. Ostermeyer M. On the implementation of a deterministic secure coding protocol using polarization entangled photons / M. Ostermeyer, N. Walenta // Optics Communications. – 2008. – V. 281, issue 17. – P. 4540–4544.

6. 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.

7. 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.

8. Василиу Е.В. Три новых протокола квантовой безопасной связи с четырехкубитными кластерными состояниями / Е.В. Василиу, Р.С. Мамедов // Цифрові технології. – 2009, № 6. – С. 94–103.

9. Василиу Е.В. Стойкость пинг-понг протокола с триплетами Гринбергера – Хорна – Цайлингера к атаке с использованием вспомогательных квантовых систем / Е.В. Василиу // Информатика: Объединенный институт проблем информатики НАН Беларуси. – 2009, № 1 (21) – С. 117–128.

10. Vasiliu E.V. Non-coherent attack on the ping-pong protocol with completely entangled pairs of qutrits / Eugene V. Vasiliu // Quantum Information Processing. – 2011. – V. 10, num. 2. – P. 189–202.

11. Василіу Є.В. Оцінки обчислювальної складності способу підсилення безпеки пінг – понг протоколу з переплутаними станами кубітів та кутритів / Є.В. Василіу, Р.С. Мамедов // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 2. – С. 14–25.

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