УДК 003.26:004.056.55:621.39

О.Г. Корченко,
доктор технічних наук, професор,
М.Г. Луцький,
кандидат технічних наук, доцент,
С.О. Гнатюк,
кандидат технічних наук

СУЧАСНІ КОМЕРЦІЙНІ СИСТЕМИ КВАНТОВОЇ КРИПТОГРАФІЇ

Обґрунтовано доцільність застосування квантових криптографічних систем для вирішення певних завдань захисту інформації. Наведено класифікацію квантових методів захисту інформації. Здійснено пошук наявних на світовому ринку систем квантової криптографії, проведено аналіз їх структурних компонентів та перспектив практичного застосування.

Ключові слова: *квантова криптографія, квантові алгоритми, квантовий розподіл ключів, квантова криптосистема, теоретико-інформаційна стійкість.*

Обоснована целесообразность применения квантовых криптографических систем для решения определенных задач защиты информации. Приведена классификация квантовых методов защиты информации. Осуществлен поиск существующих на мировом рынке систем квантовой криптографии, проведен анализ их структурных компонентов и перспектив практического использования.

Ключевые слова: *квантовая криптография, квантовые алгоритмы, квантовое распределение ключей, квантовая криптосистема, теоретико-информационная стойкость.*

In this paper the expediency of quantum cryptographic systems using for solving several information security problems is substantiated. Classification of quantum methods of information security is suggested. Search of the existing quantum cryptographic systems in the world market is carried out. Structural components of these systems and prospects of their practical implementation are analyzed as well.

Keywords: *quantum cryptography, quantum algorithms, quantum key distribution, quantum cryptographic system, information-theoretic resistance.*

Одним із найважливіших напрямів діяльності у сфері забезпечення конфіденційності даних був і залишається захист інформації (ЗІ) криптографічними методами. Розвиток систем криптографічного ЗІ, організація та налагодження виробництва вітчизняних захищених засобів і технологій обробки інформації стали пріоритетними напрямами діяльності у сфері забезпечення інформаційної безпеки як складової національної безпеки нашої держави. Такі системи в Україні використовуюся, зокрема, у банківській сфері, органах державного управління, на об'єктах, які мають стратегічне значення для економіки і безпеки держави тощо.

Симетричні криптографічні засоби є досить швидкими, проте постає проблема розподілу секретних ключів. Ця проблема, здавалося б, вирішується

асиметричними криптографічними засобами, які, проте, теж мають суттєві недоліки – вони відносно повільні, а їх криптостійкість заснована на неможливості ефективного обчислювального вирішення певного класу складних математичних задач (так званих NP-складних), наприклад, таких як факторизація та логарифмування в дискретних полях великого розміру [1]. Проте дана неможливість є не більше ніж гіпотезою, яка у будь-який момент може бути спростована, якщо буде доведене протилежне їй припущення (тобто P = NP). В іншому разі це призвело б до краху всієї сучасної криптографії, тому що задачі, на неможливості розв'язання яких вона базується, тісно пов'язані між собою і зламування навіть однієї криптосистеми буде означати неодмінний крах більшості інших. Крім того, різке збільшення продуктивності та одночасне здешевлення обчислювальних засобів робить їх загальнодоступними, чим значно розширює множину потенційних неконтрольованих загроз.

Протягом останнього десятиріччя у науково-дослідних лабораторіях усього світу проводяться активні роботи щодо створення систем (квантових комп'ютерів), заснованих на квантових обчисленнях, які орієнтуються на ефективне вирішення складних завдань. На цей час загальновідомо, що відповідні квантові алгоритми експоненціально швидше за найоптимальніші традиційні алгоритми розв'язують задачу факторизації (алгоритм Шора) і виконують швидкий пошук у невпорядкованих базах даних (алгоритм Гровера) [2], що є досить важливим при вирішенні NP-складних задач.

Усі перераховані вище чинники роблять перспективи традиційної (класичної) криптографії не повністю надійними і змушують шукати альтернативні методи забезпечення захищеності (зокрема конфіденційності) інформаційних ресурсів. Зважаючи на сучасні тенденції розвитку, такими альтернативами можуть бути методи квантової криптографії. Численні успішні експерименти доводять здатність таких методів вирішити ряд традиційних криптографічних задач, зокрема, розподіл ключів шифрування. Квантова криптографія ґрунтується на непорушності законів квантової механіки, що дає можливість досягти теоретико-інформаційної стійкості, яка не залежить від обчислювальних та інших можливостей зловмисника, – це основна перевага квантової криптографії над традиційними методами криптографії.

З огляду на це, *метою цієї роботи* є пошук існуючих квантових криптосистем, аналіз їх архітектурних особливостей та перспектив впровадження в наявні інформаційно-комунікаційні системи.

Базовими задачами криптографії є розподіл криптографічних ключів, аутентифікація сторін та авторизація легітимних користувачів. Розподіл ключів між законними користувачами в умовах суворої секретності є однією з найважливіших проблем сучасної криптографії, яка, відповідно до роботи [3], може бути вирішена за допомогою:

– *класичної теоретико-інформаційної схеми* (для її реалізації необхідний канал з перешкодами; ефективність схеми вкрай низька – 3–8 % [4]);

– *класичної криптографічної схеми з відкритим ключем* (схема Діфі-Хелмана [1, 4], схема цифрового конверта; має обчислювальну стійкість);

– *класичної симетричної криптографічної схеми з обчислювальною стійкістю* (потребує наявності в абонентів попередньо встановленого ключа, тобто може розглядатися тільки як схема для збільшення довжини ключа, а не для його розподілення) [1, 4];

– *квантового розподілу ключів* (забезпечує теоретико-інформаційну стійкість, але потребує наявності в абонентів попередньо встановленого ключа для аутентифікації класичного каналу, тобто теж може розглядатися як схема для збільшення довжини ключа);

– *методу довірених кур'єрів* (основні недоліки цього методу – висока вартість, значна залежність від людського чинника).

Наразі кількість публікацій у галузі квантової криптографії невпинно зростає, з огляду на те, що в роботі [4] була запропонована така узагальнена класифікація квантових методів захисту інформації (рис. 1):

Рис. 1. Класифікація квантових технологій захисту інформації

Крім того, у згаданій роботі наведено ґрунтовний опис більшості існуючих протоколів квантової криптографії з формалізацією вхідних і вихідних параметрів, аналізом переваг і недоліків, а також з рекомендаціями щодо підсилення секретності роботи систем захисту інформації на базі відповідних протоколів в умовах дії кіберзагроз. З огляду на це, можна зробити висновок, що саме КРК є найбільш досліджуваною квантовою технологією захисту інформації. Іншим доказом цього є те, що саме КРК ліг в основу створення усіх наявних на цей час комерційних квантово-криптографічних систем.

Першим у світі комерційним рішенням квантової криптографії була система *QPN Security Gateway (QPN-8505)* [5], запропонована компанією MagiQ Technologies (США). Ця система (рис. 2) є економічно вигідним криптографічним рішенням, зорієнтованим на урядові та фінансові організації. У цій системі MagiQ Technologies пропонує захист VPN за допомогою квантового розподілу ключів (до ста 256-бітних ключів за секунду на відстань до 140 км) та інтегрованого шифрування. Система QPN-8505 використовує такі протоколи: квантовий BB84 [4], класичні 3DES (112 біт) та AES (256 біт) [1]. За допомогою цієї системи можна організувати захищену квантову мережу, як це показано на рис. 3. Варто також відзначити, що система QPN Security Gateway для більшості потенційних клієнтів (зокрема в Україні) є важкодоступною через високу вартість (мінімальна конфігурація системи коштує близько € 80 тис. [5]).

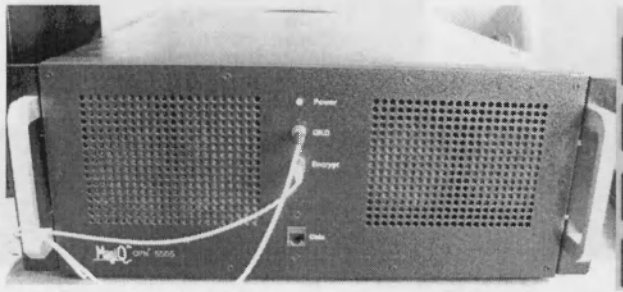

Рис. 2. Квантова криптосистема QPN-8505

Рис. 3. Варіант організації мережі на базі QPN-8505

На сьогодні в Україні подібні системи відсутні як у науково-дослідних інститутах, так і в потенційних споживачів такого продукту. Дещо краща ситуація

склалася у східних сусідів – екземпляр криптосистеми від MagiQ Technologies був представлений у науково-дослідній лабораторії квантової криптографії Таганрозького технологічного інституту ФДНЗВПО "Південного федерального університету".

Крім того, у зазначеній лабораторії є й інше обладнання, придатне для проведення практичних експериментів щодо КРК, випробування стійкості квантових криптосистем тощо, зокрема система квантового розподілу ключів *Clavis*^{2} (рис. 4) від швейцарської компанії ID Quantique [6]. Систему Clavis^2 побудовано на автокомпенсуючій оптичній платформі, завдяки чому забезпечується стабільність і низький рівень квантових помилок, що підтверджено численними експериментами. За допомогою цієї системи можна здійснювати захищений розподіл ключів шифрування між двома абонентами на відстань до 100 км. Ринкова вартість системи Clavis^2 станом на грудень 2011 року складає близько € 90 тис. [6], включаючи річну підтримку телефоном та електронною поштою, а також двотижневе навчання на базі виробника.

Крім того, компанія ID Quantique пропонує іншу квантову систему під назвою *Cerberis* [7], що являє собою сервер з автоматичним створенням і секретним обміном ключами захищеним оптоволоконним каналом (FC-1G, FC-2G та FC-4G). Ця система (рис. 5) може розподіляти криптографічні ключі на відстань до 50 км, її характерною особливістю є наявність 12 паралельних криптообчислень, що значно підвищує швидкодію. Система Cerberis використовує для шифрування протокол AES (256 біт), а для КРК – протоколи BB84 та SARG [4]. Орієнтовна вартість такої системи на ринку становить € 70 тис. [7].

Нещодавно британською компанією Toshiba Research Europe Ltd (м. Кембрідж) було представлено ще одну систему КРК під назвою *Quantum Key Server* [8]. Ця система вирізняється простотою своєї архітектури й забезпечує генерацію до ста 256-бітних ключів на секунду та їх односторонню передачу від передавача до приймача. До її складу входить інтегрований модуль автоматичного управління, що проводить неперервний моніторинг системи Quantum Key Server і регулює оптичні характеристики. Інша британська компанія QinetiQ запропонувала першу у світі комп'ютерну мережу, що використовує квантову криптографію – *Quantum Net (Qnet)* [9]. Максимальна довжина ліній зв'язку зазначеної мережі становить 120 км, та найголовнішим є те, що система Qnet – це перша квантово-криптографічна система, яка використовує більше 2 серверів. Їх у цій системі аж 6, і всі вони є інтегрованими в Internet.

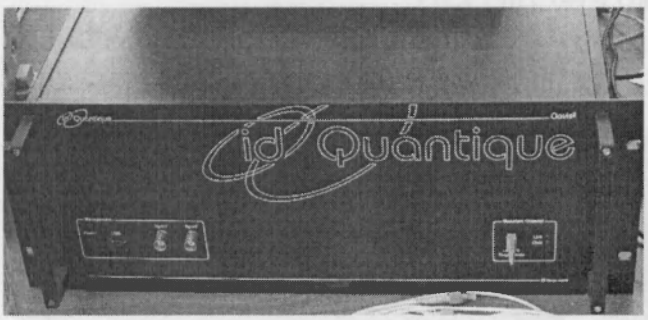

Рис. 4. Швейцарська квантова криптосистема Clavis^2

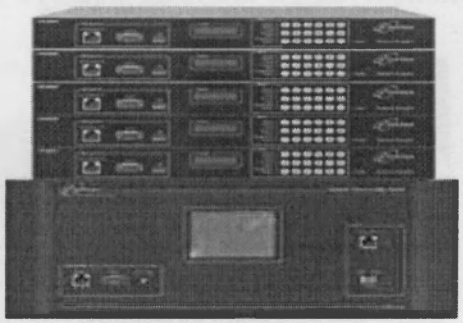

Рис. 5. Система квантової криптографії Cerberis

Вчені провідних країн світу беруть активну участь у реалізації прикладних міжнародних проектів, таких як: *SECOQC (Secure Communication based on Quantum Cryptography), EQCSPOT (European Quantum Cryptography and Single Photon*

Technologies) та *SwissQuantum* [3, 10]. Що стосується першого проекту [3], то ще у 2004 році Євросоюз вирішив інвестувати € 11 млн на розвиток квантової криптографії для протидії шпигунським діям американської системи збору інформації ECHELON. Проект стартував у Відні восени 2008 року й об'єднав вчених та організації з таких країн, як: Австрія, Бельгія, Великобританія, Канада, Чехія, Італія, Німеччина, Швеція, Данія, Швейцарія та Росія. Основною метою проекту EQCSPOT є виведення квантової криптографії на рівень промислового застосування. Основними завданнями, що вирішуються в межах цього проекту, є створення захищеного середовища вільного ключового обміну, розробка архітектурних компонентів та програмного забезпечення для квантово-криптографічних систем, а також донесення отриманих результатів до широкого кола читачів (користувачів подібних систем та ймовірних клієнтів). Базовою задачею проекту SwissQuantum є демонстрація можливостей квантово-криптографічної мережі і, хоча це не перша подібна мережа, вона єдина працює в реальних умовах і за реальним мережевим трафіком.

Також варто відзначити, що нині інтенсивно ведуться теоретичні та практичні дослідження щодо розробки квантових криптосистем відомими науково-дослідними інститутами та центрами – Institute for Quantum Optics and Quantum Information, Northwestern University, SmartQuantum, BBN Technologies of Cambridge, TREL, NEC, Mitsubishi Electric, ARS Seibersdorf Research, Los Alamos National Laboratory та ін.

Таким чином, нами наведено узагальнену класифікацію наявних квантових методів захисту інформації, проаналізовано всі загальнодоступні (відкриті) квантові криптосистеми. Як показав аналіз, основними країнами-виробниками таких систем є Великобританія, США та Швейцарія. Основною і незаперечною перевагою квантових криптосистем є розподіл ключів шифрування з теоретико-інформаційною стійкістю, що є неможливим за використання класичних криптографічних засобів. Основним же недоліком систем квантової криптографії є їхня ринкова вартість, що значно звужує коло можливих споживачів. Проте вказаний недолік не зменшує важливості квантової криптографії, а статистика засвідчує той факт, що річні втрати підприємств (у тому числі, і вітчизняних) від кіберзагроз є на порядок більшими, ніж вартість квантових криптосистем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Кузнецов Г.В.* Математичні основи криптографії : навчальний посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. – Дніпропетровськ : Національний гірничий університет, 2004. – Ч. 1. – 391 с.

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

3. SECOQC White Paper on Quantum Key Distribution and Cryptography / Romain Alleaume, Jan Bouda, Cyril Branciard [et al.]. – Preprint : http://www.arxiv.org/abs/quant-ph/0701168v1.

4. *Корченко О.Г.* Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Захист інформації. – 2010. – № 1. – С. 77–89.

5. QPN-8505 Security Gateway [Electronic resource] : Data Sheet / MagiQ Technologies, Inc. – Electronic data (1 file : 143 754 byte). – Somerville, Massachusetts, USA : MagiQ Technologies, Inc., 2007, [10.12.2011]. – Mode of access: http://www.magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf.

6. Clavis² [Electronic resource] : Quantum key distribution for r&d applications / ID Quantique SA. – Electronic data. – Geneva, Switzerland : ID Quantique SA, [10.12.2011]. – Mode of access : http ://www.idquantique.com/scientific-instrumentation/clavis2-qkd-platform.html.

7. Cerberis Encryption Solution [Electronic resource] : Layer 2 Encryption with Quantum Key Distribution / ID Quantique SA. – Electronic data. – Geneva, Switzerland : ID Quantique SA, [10.12.2011]. – Mode of access : http ://www.idquantique.com/products/cerberis.htm.

8. Quantum Key Distribution System [Electronic resource] : Toshiba Research Europe Ltd., Cambridge Research Laboratory. – Electronic data. – Tokyo, Japan : Toshiba Corporation, 2010, [10.12.2011] – Mode of access: http ://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html.

9. *Elliot C.* Quantum Cryptography in Practice / Elliot C., Pearson D, Troxel G. – Preprint : arXiv:quant-ph/0307049.

10. *Korchenko O.* Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Y. Vasiliu, S. Gnatyuk // Aviation. Vilnius : Technika, 2010, Vol. 14, № 2, pp. 58–69.

Отримано 14.11.2011