Система передачі криптографічних ключів

Сергій Гнатюк

Кафедра безпеки інформаційних технологій, Інститут інформаційно-діагностичних систем,
Національний авіаційний університет, УКРАЇНА, м.Київ, просп. Космонавта Комарова, 1, E-mail: SergiyGnatyuk@meta.ua

The proposed system of cryptographic key distribution referes to the cryptographic protection of information and can be used for secure cryptografic key distribution for their further use in encryption algorythms. The technical effect can be achieved by implementation of this system and the point is to exclude the possibility of cryptographic key interception during the process of key transmission between stations. This introdused cryptographic key distribution system is built to solve the problem of secure keys by using quantum key distribution which is based on inviolability of laws of quantum mecanics.

Cryptographic protection, information security, quantum key distribution, secret key cryptography, Heisenberg uncertainty principle, Advanced Encryption Standard, the problem of key distribution, analog-to-digital converter.

Криптографія використовує останні досягнення фундаментальних наук для створення і удосконалення схем шифрування та розшифрування інформації. Ці алгоритми відомі та відкриті, а секретність криптограм повністю залежить від секретності ключа. Проблема розподілу ключів має два варіанти вирішення – математичний, який використовується у традиційній криптографії з відкритим ключем та фізичний, що використовується у квантовій криптографії. Проте не існує жодного практичного криптографічного механізму, який гарантував би захищеність ключа під час його передачі звичайним не квантовим комунікаційним каналом [1].

Аналізуючи існуючі розробки, спрямовані на вирішення проблеми розподілу ключів, варто відмітити системи, що основані на асиметричних алгоритмах шифрування. Завданням таких систем являється збільшення кількості математичних операцій, що зробить неможливим дешифрування криптограми використовуючи існуючі обчислювальні засоби. Крім того, в останні п’ять років спостерігається поява корпоративних рішень, основаних на квантовому розподілі ключів – це, перш за все, розробки відомих світових компаній «QinetiQ», «Toshiba Research Europe», «MagiQ», «QCV» та ін. У більшості випадків дані продукти мають закриту архітектуру, що являється комерційною таємницею виробників.

Метою створення даної системи є виключення можливості перехоплення криптографічного ключа в процесі міжабонентної передачі. Для досягнення даної мети була поставлена задача розробки системи безпечної передачі криптографічних ключів, що дозволить виключити ймовірність перехоплення ключа під час його передачі від першого абонента до другого. Поставлена задача вирішується за допомогою квантового розподілу ключів, який оснований на використанні оптоволоконного каналу і передачі по ньому поляризаційних станів фотонів від одного легітимного абонента до іншого. Технічний результат полягає у виключенні можливості перехоплення криптографічного ключа в процесі міжабонентної передачі.

На рис.1 зображена структурна схема системи передачі криптографічних ключів:

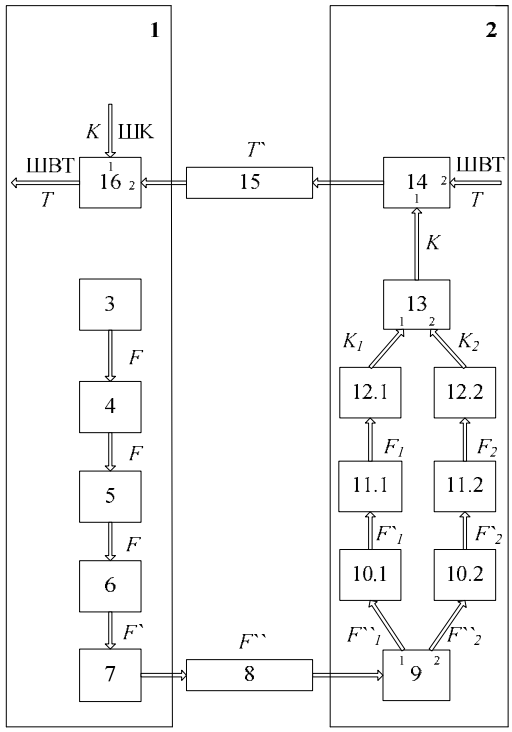

Рис. 1. Система передачі криптографічних ключів

Система передачі криптографічних ключів містить модуль 1 абонента відправника, модуль 2 абонента приймача, лазерне джерело випромінювання 3, оптичний циркулятор 4, інтерферометр Маха-Цендера 5, два волоконно-оптичні фазові модулятори 6 та 9, керуючий оптичний одномодовий атенюатор 7, захищений волоконно-оптичний канал 8, два фотодетектори 10.1 та 10.2, два напівпровідникові оптичні підсилювачі 11.1 та 11.2, два аналогово-цифрових перетворювачі 12.1 та 12.2, блок 13 конкатенації ключових повідомлень, блок 14 шифрування даних, відкритий канал 15, блок 16 дешифрування даних, шину відкритого тексту ШВТ і шину ключа ШК. Абонент 1 відправник генерує послідовність коротких оптичних імпульсів F (на довжині хвилі 1550 нм) за допомогою лазерного джерела випромінювання 3, яка надходить на вхід оптичного циркулятора 4, після цього задана послідовність надходить на вхід інтерферометра Маха-Цендера 5 для направленої передачі, вихід якого сполучений з входом волоконно-оптичного фазового модулятора 6, який здійснює фазове кодування фотонів, результатом чого на його виході з’являється послідовність F`, яка надходить на вхід керуючого оптичного одномодового атенюатора 7, що послаблює дану послідовність до рівня одиничних

фотонів і з виходу даного блоку передається у вигляді ослабленої послідовності одиничних фотонів F`` через захищений волоконно-оптичний канал 8 до абонента 2 приймача на вхід другого волоконно-оптичного фазового модулятора 9, який здійснює фазове декодування послідовності F``, таким чином, що на його першому і другому виходах з'являються послідовності F``1 та F``2 відповідно, які передаються на перший 10.1 і другий 10.2 фотодетектори відповідно (причому абонент 1 відправник та абонент 2 приймач попередньо домовились про порядок розташування детекторів), перший з яких 10.1 аналізує фотони в ортогональному, а другий 10.2 в діагональному базисах і передають послідовності F`1 та F`2 на вхід першого 11.1 і другого 11.2 напівпровідникового оптичного підсилювача відповідно, де сигнали підсилюються, щоб зменшити наслідки впливу завад, після чого з виходів 11.1 та 11.2 послідовності F1 та F2 відповідно надходять на вхід першого і другого аналогово-цифрового перетворювача 12.1 та 12.2, на виході яких з'являються цифрові двійкові послідовності К1 та К2, які передаються відповідно на перший та другий вхід блоку 13 конкатенації ключових повідомлень, на виході якого формується єдина двійкова ключова послідовність К, що надходить на перший вхід блоку шифрування даних 14, на другий вхід якого через шину ШВТ надходить вхідне повідомлення Т і в результаті здійснення шифрування за загальновідомим симетричним алгоритмом AES [2] на виході блоку 14 з'являється зашифрована послідовність Т`, яка передається відкритим каналом 15 на другий вхід блоку дешифрування 16, на перший вхід якого через шину ключа ШК подається двійкова ключова послідовність К і, в результаті здійснення дешифрування вищезгаданим загальновідомим симетричним алгоритмом, на виході блоку 16 отримуємо дешифроване повідомлення Т, яке передається на шину ШВТ.

Основними принципами квантової механіки, що лежать в основі системи, являються:

- принцип невизначеності Гейзенберга, згідно якого неможливо провести вимірювання в квантовій системі, не змінивши її – це дозволяє детектувати будь-які втручання в систему з боку третіх осіб;
- неможливість одночасного вимірювання взаємодоповнюючих параметрів системи – тобто зловмисник не може одночасно виміряти хвильові та корпускулярні властивості системи – це значно зменшує ймовірність перехоплення повідомлення;
- неможливо з абсолютною точністю одночасно виміряти поляризацію фотона в ортогональному та діагональному базисах – збільшує кількість помилок при спробі втручання і вимірювання на 50%;
- «теорема про неможливість клонування квантових станів» [3], яка вказує на неможливість копіювання довільного квантового стану з боку зловмисника – це унеможливлює створення точних копій станів фотонів за умов використання будь-якого обладнання.

У сукупності вищеперераховані ознаки роблять можливим досягнення вищезгаданого технічного результату. Проте при практичній реалізації виникають інші проблеми, на вирішення яких можуть бути спрямовані наступні дослідження – це обмеження довжини квантового каналу через неможливість його підсилення без втрат квантових властивостей та проблема аналізу одиничних фотонів під впливом шуму.

References

[1] Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С.П. Кулик, Е.А. Шапиро (пер. с англ.); С.П.Кулик, Т.А. Шмаонов (ред.пер.); Д. Боумейстер и др. (ред.). – М.: Постмаркет, 2002. – с. 33-73

[2] NIST. "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at http://csrc.nist.gov/publications/fips/

[3] Wooters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. – 1982. – Vol. 299. – P. 802.