



УКРАЇНА

(19) UA (11) 43779 (13) U
(51) МПК (2009)
H04L 9/08

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СИСТЕМА ПЕРЕДАЧІ КРИПТОГРАФІЧНИХ КЛЮЧІВ

1

(21) u200904239

(22) 29.04.2009

(24) 25.08.2009

(46) 25.08.2009, Бюл.№ 16, 2009 р.

(72) ГНАТЮК СЕРГІЙ ОЛЕКСАНДРОВИЧ, КІН-
ЗЕРЯВИЙ ВАСИЛЬ МИКОЛАЙОВИЧ, КОРЧЕНКО
ОЛЕКСАНДР ГРИГОРОВИЧ, ПАЦІРА ЄВГЕНІЯ
ВІКТОРІВНА(73) НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИ-
ТЕТ

(57) 1. Система передачі криптографічних ключів, що містить модуль абонента відправника і модуль абонента приймача, яка **відрізняється** тим, що додатково введено відкритий канал і захищений волоконно-оптичний канал, причому вихід модуля абонента приймача підключений до входу відкритого каналу, вихід якого з'єднаний із входом модуля абонента відправника, вихід якого підключений до входу захищеного волоконно-оптичного каналу, вихід якого з'єднаний із входом модуля абонента приймача.

2. Система передачі криптографічних ключів за п. 1, яка **відрізняється** тим, що модуль абонента відправника містить блок дешифрування даних, шину ключа, шину відкритого тексту, лазерне джерело випромінювання, оптичний циркулятор, інтерферометр Маха-Цендера, волоконно-оптичний фазовий модулятор і керуючий оптичний одномодовий атенюатор, причому шина відкритого тексту підключена до виходу блоку дешифрування даних, перший вхід якого з'єднаний з шиною ключа, а другий вхід якого підключений до входу абонента відправника, вихід якого з'єднаний з виходом керуючого оптичного одномодо-

2

вого атенюатора, вхід якого підключений до виходу волоконно-оптичного фазового модулятора, вхід якого з'єднаний з виходом інтерферометра Маха-Цендера, вхід якого підключений до виходу оптичного циркулятора, вхід якого підключений до виходу лазерного джерела випромінювання.

3. Система передачі криптографічних ключів за п. 1, яка **відрізняється** тим, що модуль абонента приймача містить шину відкритого тексту, два фотодетектори, два напівпровідникових оптичних підсилювачі, два аналогово-цифрових перетворювачі, волоконно-оптичний фазовий модулятор, блок конкатенації ключових повідомлень, блок шифрування даних, причому вхід модуля абонента приймача з'єднаний із входом волоконно-оптичного фазового модулятора, перший вихід якого підключений до входу першого фотодетектора, вихід якого з'єднаний із входом першого напівпровідникового оптичного підсилювача, вихід якого підключений до входу першого аналого-цифрового перетворювача, вихід якого з'єднаний із першим входом блока конкатенації ключових повідомлень, другий вхід якого підключений до виходу другого аналого-цифрового перетворювача, вхід якого з'єднаний із виходом другого напівпровідникового оптичного підсилювача, вхід якого підключений до виходу другого фотодетектора, вхід якого з'єднаний з другим виходом волоконно-оптичного фазового модулятора, а вихід абонента приймача підключений до виходу блоку шифрування даних, перший вхід якого з'єднаний з виходом блока конкатенації ключових повідомлень, другий вхід якого підключений до шини відкритого тексту.

Запропонована корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана для безпечного розподілу криптографічних ключів з метою їх подальшого використання у відомих схемах шифрування.

Алгоритми шифрування і розшифрування відомі та відкриті, а секретність криптограми повністю залежить від секретності ключа. Проблема розподілу ключів має два варіанти вирішення - математичний, який використовується у традиційній

(13) U
(11) 43779
(19) UA

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].

Відома криптографічна система захисту інформації [2] містить станцію відправника і станцію одержувача, з'єднані між собою вільним від помилок каналом для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача і вільним від помилок каналом для передачі допоміжних даних від станції одержувача до станції відправника, причому станція відправника містить генератор (засіб зберігання) початкової інформаційної послідовності, вихід якого з'єднаний з входом кодера, а станція одержувача містить декодер і блок зберігання. Дана система захисту інформації призначена для формування спільного секретного ключа двома користувачами відкритого каналу і головним її недоліком є те, що абсолютна секретність (теоретична стійкість) забезпечується лише за умови, що канал криптоаналітика більш зашумлений ніж канал законних користувачів, що на практиці не завжди може бути дотримано. Крім того, подальше використання, отриманого таким чином, секретного ключа в криптографічних системах не виключає їх розкриття з використанням диференціального та лінійного криптоаналізу (зважаючи на потужність сучасних комп'ютерних засобів аналізу).

Найбільш близьким, до запропонованого технічним рішенням, обраним як прототип, є криптографічна система для захисту інформації [3], яка має станцію відправника і станцію одержувача, з'єднані між собою вільним від помилок каналом для передачі допоміжних даних від станції одержувача до станції відправника, причому станція відправника містить генератор початкової інформаційної послідовності, вихід якого з'єднаний з входом кодера, а станція одержувача містить декодер і блок зберігання, канал для передачі допоміжних даних від станції одержувача до станції відправника є каналом з перешкодами, станція відправника містить перший суматор за модулем 2, перший вхід якого з'єднаний з виходом згаданого кодера, який є кодером комбінованого кодування, другий - з виходом каналу для передачі допоміжних даних від станції одержувача до станції відправника, а вихід - з входом каналу для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача, лінію затримки і другий суматор за модулем 2, причому вихід генератора випадкової послідовності підключений до входу каналу для передачі допоміжних даних від станції одержувача до станції відправника і до входу лінії затримки, вихід якої з'єднаний з першим входом другого суматора за модулем 2, другий вхід якого з'єднаний з виходом каналу для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача, а вихід - з входом декодера, який є декодером комбінованого декодування, вихід якого підключений до входу блока зберігання.

Кодер комбінованого кодування містить послідовно з'єднані кодер випадкового кодування і кодер перешкодостійкого кодування, причому вхід кодера випадкового кодування є входом кодера комбінованого кодування, а вихід кодера перешкодостійкого кодування - виходом кодера комбінованого кодування, декодер комбінованого декодування містить послідовно з'єднані декодер перешкодостійкого декодування і декодер невинипадкового декодування, причому вхід декодера перешкодостійкого декодування є входом декодера комбінованого декодування, а вихід декодера невинипадкового декодування - виходом декодера комбінованого декодування.

Кодер комбінованого кодування містить послідовно з'єднані кодер перешкодостійкого кодування і кодер випадкового кодування, причому вхід кодера перешкодостійкого кодування є входом кодера комбінованого кодування, а вихід кодера випадкового кодування - виходом кодера комбінованого кодування, декодер комбінованого декодування містить послідовно з'єднані декодер невинипадкового декодування і декодер перешкодостійкого декодування, причому вхід декодера невинипадкового декодування є входом декодера комбінованого декодування, а вихід декодера перешкодостійкого декодування - виходом декодера комбінованого декодування. Вільний від помилок канал для передачі закодованої інформаційної послідовності від станції відправника до станції одержувача має на своєму вході каналний кодер перешкодостійкого кодування, а на виході - каналний декодер перешкодостійкого декодування.

Дана криптографічна система для захисту інформації хоча й забезпечує теоретичну стійкість без використання секретного ключа, проте не виключає ймовірність перехоплення інформаційної послідовності зловмисником (відповідно не виключається ймовірність його подальшого аналізу). До того ж, при практичній реалізації даної системи виникає ще одна проблема - необхідність створення і передачі великого секретного коду, необхідного кожен раз, коли відправляється нове повідомлення. Тому дана криптографічна система для захисту інформації не повністю вирішує задачу передачі інформації між двома абонентами в умовах секретності.

Метою даної корисної моделі 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 фізичного каналу (оптоволоконного) і передачі по ньому поляризаційних станів фотонів від одного абонента до іншого.

Технічний результат, який може бути отриманий при створенні корисної моделі полягає у виключенні можливості перехоплення крипто-

графічного ключа в процесі міжабонентної передачі.

Сутність запропонованої системи передачі криптографічних ключів полягає в тому, що задача безпечної передачі ключів вирішується за допомогою квантового розподілу ключів, який оснований на непорушності законів квантової механіки.

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» [4], яка вказує на неможливість копіювання довільного квантового стану з боку зловмисника - це унеможливорює створення точних копій станів фотонів за умов використання будь-якого обладнання. В сукупності вищеперераховані ознаки роблять можливим досягнення даного технічного результату.

На Фіг. зображена структурна схема системи 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 атенуатор 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.

У загальному вигляді система передачі криптографічних ключів працює наступним чином. 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 атенуа-

тора 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 F_1 та F_2 відповідно надходять на вхід першого і другого аналогово-цифрового перетворювача 12.1 та 12.2, на виході яких з'являються цифрові двійкові послідовності K_1 та K_2 , які передаються відповідно на перший та другий вхід блоку 13 конкатенації ключових повідомлень, на виході якого формується єдина двійкова ключова послідовність K , що надходить на перший вхід блоку шифрування даних 14, на другий вхід якого через шину ШВТ надходить вхідне повідомлення T і в результаті здійснення шифрування за загальновідомим симетричним алгоритмом AES [5] на виході блоку 14 з'являється зашифрована послідовність T' , яка передається відкритим каналом 15 на другий вхід блоку дешифрування 16, на перший вхід якого через шину ключа ШК подається двійкова ключова послідовність K і, в результаті здійснення дешифрування вищезгаданим загальновідомим симетричним алгоритмом, на виході блоку 16 отримуємо дешифроване повідомлення T , яке передається на шину ШВТ.

Джерела інформації:

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. Патент США №5161244 (аналог).

3. Горицький В.М., Полозюк О.М., Зубченко А.П. Спосіб криптографічного захисту інформації і криптографічна система для його здійснення. Пат. UA 61612A, МПК (2006) H04L9/00. - №2003032304; Заявл. 17.03.2003; Опубл. 17.11.2003, Бюл. №11, 2003р. (прототип).

4. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. - 1982. - Vol. 299. - P.802.

5. NIST. "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at <http://csrc.nist.gov/publications/fips/>.

