© Ryabyy M. Review of current methods of quantum and post-quantum cryptography // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 236-241.

ОГЛЯД СУЧАСНИХ МЕТОДІВ КВАНТОВОЇ ТА ПОСТ-КВАНТОВОЇ КРИПТОГРАФІЇ

Мирослав Рябий

Європейський університет, Україна

РЯБИЙ Мирослав Олександрович, к.т.н.

Рік та місце народження: 1987 рік, с. Салиха, Київська область, Україна.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: завідувач кафедри організації комплексного захисту інформації з 2013 року.
Наукові інтереси: інформаційна безпека, криптографія, квантова криптографія.
Публікації: більше 40 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях, патенти.
E-mail: m.ryabyy@ukr.net

Анотація. *Квантовий комп'ютер може зруйнувати більшість, якщо не всі традиційні криптосистеми, що використовуються на практиці, а саме, всі системи на основі задачі факторизації цілих чисел (наприклад RSA) або завдання дискретного логарифмування (як традиційних, так і на еліптичних кривих Діффі-Хеллмана і DSA; а також всю криптографію, засновану на спаровуваннях). Деякі класичні криптосхеми, що базуються на обчислювально-складних завданнях, сильно відрізняються від зазначених вище і їх набагато складніше вирішити, вони залишаються незалежними від квантових обчислень. У даній роботі проведено огляд методів захисту інформації на базі квантових та пост-квантових технологій. Для кожного з методів захисту інформації на базі квантових технологій наведено переваги та недоліки. Описано системи пост-квантової криптографії на основі теорії ґраток. Результати проведеного огляду дозволяють формалізувати напрями подальших досліджень пост-квантових методів та розробки нових ефективних систем захисту інформації з використанням квантових технологій.*

Ключові слова: *захист інформації, квантова криптографія, пост-квантова криптографія, квантовий розподіл ключів, квантовий комп'ютер, криптографія на основі теорії ґраток.*

Вступ

Основним завданням криптографії було виключно забезпеченням конфіденційності повідомлень (тобто шифруванням) — перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотне відновлення на стороні одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав без секретного ключа, необхідного для дешифровки повідомлення. З часом сфера застосування криптографії розширилася і включає не лише таємну передачу повідомлень, але і методи перевірки цілісності повідомлень, ідентифікації відправника / одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження, та технології безпечного спілкування тощо [1].

На початку XXI ст. було виявлено тісний взаємозв'язок між інформатикою та фізикою. Успіх у вирішенні багатьох завдань, які на перший погляд мали відношення лише до інформаційних технологій та захисту інформації, може бути досягнутий суто фізичним шляхом. Після чого перед вченими стало два питання: наскільки великі можливості квантових алгоритмів; чи можливе створення пристроїв, що реалізують ці алгоритми.

У 60-ті роки XX ст., коли бурхливими темпами почали розвиватися інформаційні технології та обчислювальна техніка, зародилася нова наука - квантова теорія інформації. Вона вивчає квантово-механічні стани і їх здатність брати участь у процесі перенесення і обробки інформації. Квантова теорія є математичною моделлю сучасного уявлення про фізичні властивості навколишнього світу і фізичних систем, з яких він складається [2].

Сьогодні квантовий комп'ютер може зруйнувати більшість, якщо не всі традиційні криптосистеми, що використовуються на практиці, а саме, всі системи на основі задачі факторизації цілих чисел (наприклад RSA) або завдання дискретного логарифмування (як традиційних, так і на еліптичних кривих Діффі-Хеллмана і DSA; а також всю криптографію, засновану на спаровуваннях). Хоча існують механізми класичної криптографії, які не піддаються дії квантових комп'ютерів. Деякі класичні криптосхеми, що базуються на обчислювально-складних завданнях, сильно відрізняються від зазначених вище і їх набагато складніше вирішити, вони залишаються незалежними від квантових обчислень. Термін «пост-

квантова криптографія» був запропонований Д. Бернштейном і вже став загальноприйнятим в криптографічній літературі. Він позначає ту частину криптографії, що залишилася після появи квантових комп'ютерів і квантових атак.

Аналіз існуючих досліджень

У роботі [3] проведено аналіз сучасних квантових технологій захисту інформації, а в праці [4] розглянуто сучасний стан квантової криптографії, показаний її внесок у вирішення проблем сучасної криптологічної науки. У роботі [5] розроблено методи синтезу досконалих багаторівневих алгебраїчних конструкцій – досконалих багаторівневих ґраток (ДБГ) та запропоновано регулярні правила їх побудови, досліджено структурні та кореляційні властивості ДБГ і запропоновано регулярні правила їх розмноження. У роботі [6] для синтезу продуктивних алгоритмів розподілу відкритих ключів і відкритого шифрування вводиться нова обчислювально-складна задача над скінченними не комутативними групами. Запропоновано підхід до побудови не комутативних груп чотиривимірних векторів над простим полем і виводиться формула для порядку цих груп. Описана схема узгодження загального секретного ключа двох віддалених абонентів і алгоритм відкритого шифрування на основі нового складного завдання. Проте, в роботі [7] наводиться криптоаналіз запропонованого розподілу ключів, що доводить – верхня оцінка криптографічної стійкості розглянутої криптосистеми відкритого розподілу ключів по порядку не перевищує складності проблеми дискретного логарифмування в циклічній підгрупі порядку q мультиплікативної групи поля Z_p або його квадратичному розширенні, де q - простий дільник відповідно чисел p-1 або p+1.

До теперішнього часу запропоновано багато квантових технологій захисту інформації, що відрізняються як основними принципами, покладеними в їх основу, так і ступенем їх надійності, а також методами практичної реалізації. Також, класична криптографія (пост-квантова) продовжує свій розвиток в криптографії, що базується на основі теорії ґраток та криптосистемах, що базуються на синдромах. Метою є пошук методів квантової та пост-квантової криптографії, визначення їхніх переваг та недоліків, а також перспектив практичної реалізації.

Основна частина дослідження

До складу квантових технологій захисту інформації входить [3]: передавання інформації за допомогою одиночних кубітів; передавання інформації за допомогою багаторівневих квантових систем (кудитів); передавання інформації за допомогою квантових кореляцій. До методів захисту інформації на базі квантових технологій входять (рис. 1) [3]: квантовий розподіл ключів [4, 8-17], квантовий прямий безпечний зв'язок [4, 18-23], квантове розділення секрету [24-26], квантовий потоковий шифр [27, 28], квантовий цифровий підпис [29-32] та квантова стеганографія [33-35]. Переваги та недоліки вище зазначених методів наведено в табл. 1.

Таблиця 1

Переваги та недоліки методів захисту інформації на базі квантових технологій

Методи захисту інформації на базі квантових технологій	*Переваги*	*Недоліки*
Квантовий розподіл ключів		
Протоколи з використанням одиночних поляризованих фотонів (protocols using single polarized photons): BB84, SARG, протокол з 6-ма станами, протокол "4+2", протокол Гольденберга-Вайдмана, протокол Коаші-Імото та ін.	забезпечення теоретико-інформаційної стійкості та достовірне виявлення факту підключення зловмисника	висока ринкова ціна систем
Протоколи із застосуванням фазового кодування (protocols using phase coding): B92 та його різні варіанти		
Протоколи з використанням переплутаних станів (protocols using entangled states): протокол Екерта та різновиди протоколів з використанням переплутаних станів для багатовимірних квантових систем		
Протоколи зі станами «приманки» (decoy states protocols)		
Квантовий прямий безпечний зв'язок		
Пінг-понг протокол (ping-pong protocol): класичний протокол (оригінальний) та його різні варіанти з передаванням кубітів та багаторівневих квантових систем	забезпечення теоретико-інформаційної стійкості та відсутність необхідності розподілу секретних ключів	складність практичної реалізації, потреба у квантовій пам'яті великого об'єму для усіх учасників зв'язку
Протоколи з передаванням одиночних кубітів (protocol using single qubits transfer)		
Протоколи з передаванням переплутаних кубітів блоками (protocols using block transfer of entangled qubits)		
Квантовий цифровий підпис		
Протоколи з одиничними фотонами	теоретико-інформаційна захищеність та спрощена система розподілу ключів	складність практичної реалізації, генерування обмеженої кількості копій відкритого ключа та на відміну від ідеальної класичної односторонньої функції, завжди є витік певної кількості інформації про вхідні дані квантової необоротної функції
Протоколи на базі квантових кореляціях ГХЦ		

Закінчення таблиці 1

Квантовий потоковий шифр		
Протокол Yuen 2000 (Y-00)	висока швидкість шифрування даних, стійкість до швидких кореляційних атак та більша захищеність порівняно із звичайними потоковими шифрами	складність практичної реалізації
Квантова стеганографія		
Приховування у квантовому шумі	теоретичні дослідження у даній галузі ще не вийшли на рівень практичного застосування	
Приховування із застосуванням квантових завадостійких кодів		
Приховування у форматах даних, протоколах тощо		
Квантове розділення секрету		
Протокол Hillery-Buzek-Berthiaume	дозволяють виявити підслуховування та не потребують шифрування повідомлень	потреба у наявності великої квантової пам'яті в усіх сторін, що поки знаходиться за межами можливостей сучасних технологій
Протокол квантового розділення секрету з використанням одиночних фотонів блоками		

Після появи квантового комп'ютера задачі криптоаналізу класичних методів криптографії значно спростилися. Проте, класичні криптосхеми, що базуються на обчислювально-складних завданнях залишаються незалежними від квантових обчислень.

У 1996 р. угорський математик-дослідник IBM Міклос Айта в своїй роботі [36] показав, що [37]:

– можливо, побудувати одностороннюю функцію на основі SVP-завдання, по базису ґратки, знайти найкоротший ненульовий вектор (shortest vector problem, SVP); пізніші дослідники поліпшили результат до односторонньої функції з секретом (trapdoor function) - варіантом односторонньої функції, швидко обертаємої (по порівняно з швидкістю отримання образу функції) за наявності додаткових відомостей;

– переформулювання в імовірнісний варіант задачі про ранець, SVP-задача не має імовірнісного поліноміального алгоритму рішення, тобто не розв'язується за поліноміальний час на квантових комп'ютерах;

– серед усього класу NP-задач, SVP-задача є найскладнішою, тобто є NP-повним завданням.

Результати Айтая, а також невдалі спроби реалізації квантових алгоритмів розв'язання задач теорії ґраток, за аналогією з запропонованим Шором в 1987 р., ефективним мультиблочним редукційним доповненням [38] до поліноміального алгоритму L^3 або LLL [39], Ленстра, Ленстра і Ловас, що дозволяє наближено вирішувати SVP та близьких до них задач з довільно заданою точністю, зробили ці задачі найбільш ймовірними претендентами на реалізацію криптостійких до квантових систем шифрування.

Всі криптографічні системи теорії ґраток можна умовно розділити на два типи:

– які мають чітко доведену крипостійкість, але не ефективні за часом виконання алгоритму зашифрування / розшифрування та/або характеризуються швидким зростанням публічного та приватного ключів від ключових параметрів шифрування, наприклад розмірності ґратки. До таких систем шифрування відносять криптографію на основі: SVP, uSVP, SIVP - задач;

– ефективні за часом зашифрування / розшифрування і затратам на зберігання відкритого і приватного ключів, що не володіють чітко доведеною криптостійкістю. До таких систем прийнято відносити системи, засновані на деяких часткових в параметричному сенсі випадках задач теорії ґраток або ж заснованих на ґратках з циклічністю що утворює їх базис. До таких, відносять NTRU (Draft standard IEEE 1363.1) шифрування [40].

NTRU система шифрування заснована на завданні NTRU-згортки модулярних ґраток (NTRU Convolution modular lattice, NTRU CML), яка є окремим випадком CVP-задачі. Основою шифрування є операція згортки на кільці модулярних многочленів (з цілими коефіцієнтами). Під згорткою многочленів в даному випадку розуміють, їх множення, із заданим правилом згортки $x^i = 1$, де $i = const$.

На сьогоднішній день саме ця система отримала найбільше застосування серед всіх систем шифрування на основі теорії ґраток. Причиною цього є висока продуктивність алгоритму, в поєднанні з малим розміром публічного та приватного ключів (табл. 2) [41]. Основним недоліком NTRU шифрування є відсутність теоретичного обґрунтування криптостійкості, представлена в табл. 2 [41] оцінка є експериментальною, заснованої на найшвидшому варіанті алгоритму редукції ґраток - блочному алгоритмі Коркина-Золотарева (block Korkin-Zolotarev, BKZ-LLL).

Однією з найбільш досліджуваних систем шифрування на основі задач теорії ґраток є версія шифрування Айтая-Дворка (Ajtai-Dwork) позбавлена помилок розшифрування повідомлення, запропонована Голдштейном, Голдвассером і Халеві (GGH) [42] - AD_{GGH}, заснована на uSVP-задачах. Основним недоліком системи шифрування AD_{GGH}, є швидке зростання розмірів публічного і приватних ключів залежно від розмірності базису ґратки (табл. 2) [41], що ускладнює практичне застосування цієї системи.

Асиметричне шифрування Реджева ($Regev_{05}$) засновано на LWE-задачі із чітким доказом криптостійкості і поєднує в собі відносно високу швидкість зашифрування / розшифрування, а також порівняно компактні публічний і приватні ключі (табл. 2) [41].

У червні 2009 року Крейг Джентрі [43] продемонстрував реалізацію гомоморфного шифрування на ідеальних ґратках [41] для операцій додавання і множення ($\text{Gentry}_{\text{mrf}}$). Гомоморфне шифрування передбачає гомоморфізм щодо деякої операції між вихідними даними і зашифрованою інформацією. Такий тип шифрування дозволяє реалізовувати обробку зашифрованих даних (пошук по полях) без необхідності їх повної розшифровки, що забезпечує конфіденційність інформації збереженої на віддалених серверах, у тому числі при обміні даними по незахищеному каналу мережі Internet. Гіпотеза про можливості гомоморфного шифрування була запропонована Рональдом Рівестом чверть століття тому, але після марних спроб реалізації, він припустив принципову неможливість побудови таких систем.

Таблиця 2

Порівняльний аналіз систем шифрування на основі ґраток [41]

Система шифрування	*Складність параметра*			
	Криптостійкість	*Розмір публічного ключа*	*Розмір приватного ключа*	*Шифрування, розшифрування*
AD_{GGH}	$O(n^{11}) - uSVP$	$O(N^5 \log N)$	$O(N^2)$	$\approx O(n^{\log_2 c}), c < 3$
Regev_{05}	$\tilde{O}(n^{1.5}) - SVP$	$O(N^2 \log^2 N)$	$O(N \log N)$	$\tilde{O}(n)$
$\text{Gentry}_{\text{mrf}}$	$2^k - SIVP$	$\tilde{O}(k^{3.5})$	$\tilde{O}(k)$	$\tilde{O}(k^7)$
NTRU	$10^{0.0826n-2.58}$ *сек.*	$\approx \frac{1}{2} N \log_2 \frac{N}{4}$	$\approx \frac{N(n-k)\log_2 \frac{N}{4}}{2n \log_p q}$	$O(n^2)$

де n – розмір ґратки, N – об'єм базису ґратки в бітах, k – рівень захищеності в бітах відносно симетричного алгоритму шифрування, p – малий модуль, q – великий модуль.

Висновки

Отже, комерційні рішення в галузі квантових технологій захисту інформації існують лише в такому методі, як квантовий розподіл ключів, які потім використовують для класичного симетричного шифрування, та квантовий прямий безпечний зв'язок, який реалізовано в лабораторних умовах, що свідчить про появу з часом комерційних рішень. Хоча інші методи та засоби квантової криптографії є запатентованими [45-52] у різних країнах світу і мають перспективу бути реалізованими уже в найближчому майбутньому.

Також, на даний час теоретичні аспекти безпеки квантової криптографії є дуже активною галуззю досліджень, що постійно розвивається, перешкодою для них залишаються технологічні складності, що можуть бути усунені у найближчому майбутньому.

Пост-квантові системи розвиваються набагато повільніше, однією із причин є те, що існує протиріччя «крипостійкі теоретично» і «крипостійкі практично» між системами асиметричного шифрування на основі задач теорії ґраток, що відкриває перспективний напрямок фундаментальних і прикладних математичних досліджень в галузі пост-квантової криптографії.

Література

[1] Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография. — М.: Изд-во МГУ им. М.В. Ломоносова. — 2006. — С. 23–40.

[2] Постулаты квантовой теории. — ВГУ. — 2012. URL: http://www.rec.vsu.ru/rus/ecourse/quantcomp/ sem2.pdf (дата обращения 18.10.2013).

[3] Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.

[4] Василиу Е.В., Воробиенко П.П. Проблемы развития и перспективы использования квантово-криптографических систем // Наук. праці ОНАЗ ім. О.С. Попова. — 2006, № 1. — С. 3-17.

[5] Чечельницький В.Я. Методология повышения эффективности телекоммуникационных систем на основе интеграции канального кодирования и шифрования данных / В. Я. Чечельницький : дис. ... доктора техн. наук : 05.12.02 // Одеса : Одеський національний політехнічний університет, 2013. — 407 с.

[6] Молдовян Д.Н. Примитивы криптосистем с открытым ключом: конечные некоммутативные группы четырехмерных векторов // Информационно-управляющие системы. — 2010. — № 5. — С. 43–50.

[7] Глухов М.М. К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах // Матем. вопросы криптографии. — 2010. — Т. 1. — Вып. 4. — С. 5-22

[8] Bennett C.H., Bessette F., Brassard G. et al. Experimental Quantum Cryptography // Journal of Cryptography. — 1992. — V. 5. — № 1. — C. 3-28.

[9] Bennett C.H., Brassard G. Quantum cryptography: public key distribution and coin tossing // Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. — Bangalore, India. — 1984. — P. 175-179.

[10] 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.

[11] Слепов Н. Квантовая криптография: передача квантового ключа. Проблемы и решения // Электроника: НТБ. — 2006, №2. — С. 54-61.

[12] Румянцев К.Е., Голубчиков Д.М. Квантовая криптография: принципы, протоколы, системы

/ Всероссийский конкурсный отбор обзорно-аналитических статей по приоритетному направлению «Информационно-телекоммуникационные системы». — 2008. — 37 с.

[13] Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Review of Modern Physics. — 2002. — V. 74. — P. 145-195.

[14] Гиршов Е. Доклад «Введение в квантовую криптографию» (основные понятия, протоколы, примеры, технологические аспекты) // <http://www.teormin.ifmo.ru/courses/intro/38.pdf>.

[15] Cerf N.J., Bourennane M., Karlsson A., Gisin N. Security of quantum key distribution using d-level systems // Physical Review Letters. — 2002. — V. 88, №12. — 127902.

[16] Василиу Е.В., Мамедов Р.С. Сравнительный анализ эффективности и стойкости к некогерентным атакам квантовых протоколов распределения ключей с передачей многомерных квантовых систем // Наукові праці ОНАЗ ім. О.С. Попова. — 2008, № 2. — С. 20-27.

[17] Bruss D. Optimal Eavesdropping in Quantum Cryptography with Six States // Physical Review Letters. — 1998. — V. 81, № 14. — P. 3018-3021.

[18] Chuan W., Fu Guo D., Gui Lu L. Multi-step quantum secure direct communication using multi-particle Greenberg-Horne-Zeilinger state. — Optics Communications. —2005. — V. 253. — P. 15-19.

[19] Bostrom K., Felbinger T. Deterministic secure direct communication using entanglement // Physical Review Letters. — 2002. — V. 89, № 18. — 187902.

[20] Cai Q.-Y., Li B.-W. Improving the capacity of the Bostrom – Felbinger protocol // Physical Review A. — 2004. — V. 69, № 5. — 054301.

[21] Василиу Е.В., Василиу Л.Н. Пинг – понг протокол с трех– и четырехкубитными состояниями Гринбергера – Хорна – Цайлингера // Труды Одесского политехнического университета. — 2008. — Вып. 1(29). — С. 171-176.

[22] Wang Ch., Deng F.-G., Li Y.-S. et al. Quantum secure direct communication with high dimension quantum superdense coding // Physical Review A. — 2005. — V. 71, № 4. — 044305.

[23] Василиу Е.В., Мамедов Р.С. Анализ атаки пассивного перехвата на пинг-понг протокол с полностью перепутанными парами кутритов // Восточноевропейский журнал передовых технологий. — 2009, № 4/2 (40). — С. 4–11.

[24] Qin S.-J., Gao F., Zhu F.-Ch. Cryptanalysis of the Hillery-Buzek-Berthiaume quantum secret-sharing protocol // Physical Review A. — 2007. — V. 76, № 6. — 062324.

[25] Li Q., Chan W. H., Long D-Y. Semi-quantum secret sharing using entangled states // arXiv:quant-ph/0906.1866v3.

[26] Zhang Z. J., Li Y., Man Z. X. Multiparty quantum secret sharing // Physical Review A. — 2005. — V. 71, №4. — 044301.

[27] Hirota O., Sohma M., Fuse M., Kato K. Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme // Physical Review A. — 2005. — V. 72, № 2. — 022335.

[28] Nair R., Yuen H. P. On the Security of the Y-00 (AlphaEta) Direct Encryption Protocol // arXiv:quant-ph/0702093v2.

[29] Wang J., Zhang Q., Tang C. Quantum signature scheme with single photons // Optoelectronics Letters. — 2006. — V. 2, N. 3. — P. 209-212.

[30] Xiao-Jun W., Yun L. Authentic Digital Signature Based on Quantum Correlation // arXiv:quant-ph/0509129v2.

[31] Gottesman D., Chuang I. Quantum digital signatures // arXiv:quant-ph/0105032v2.

[32] Holevo A. S. Problems in the mathematical theory of quantum communication channels // Report of Mathematical Physics. — 1977. — V. 12, №2. — P. 273-278.

[33] Quantum Computation and Information. From Theory to Experiment / Imai H., Hayashi M. (eds.). — Springer-Verlag: Berlin, Heidelberg, 2006. — P. 235.

[34] Curty M., Santos D.J. Quantum steganography // In 2nd Bielefeld Workshop on Quantum Information and Complexity. — 2000. — Bielefeld, Germany. — P. 12.

[35] Pat. № 7539308 USA, H04K 1/00 (20060101). Quantum steganography / Conti, Ralph, Kenneth et al — 21.05.2004.

[36] Ajtai M. Generating Hard Instances of Lattice Problem. Proc. of 28th ACM Symp. on Theory of Comp. Philadelphia: ACM Press, 1996. — P. 99-108.

[37] Шокуров А.В., Кузюрин Н.Н., Фомин С.А. Курс лекций «Решетки, алгоритмы и современная криптография» [Електронний ресурс] - 2008. - 127 с. // <http://discopal.ispras.ru/ru.lectures-lattice-based-cryptography.htm>

[38] Schnorr C. P. A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science. — 1987. — 53(2-3). — P.201-224.

[39] Lenstra A.K., Lenstra H. W., Lovasz L. Factoring polynomials with rational coefficients. Math. Ann. — 1982. — 261(4). — P. 515-534.

[40] Hoffstein J., Pipher J., Silverman J. H. NTRU: A ring-based public key cryptosystem. In ANTS-III, 1998. — P. 267-288.

[41] Усатюк В.С. Обзор систем ассиметричного шифрования на основе задач теории решеток криптостойких к квантовым вычислительным машинам. - Братск : Братский государственный университет.

[42] Goldreich O., Goldwasser S., Halevi S. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In CRYPTO '97. —1997. — P. 105–111.

[43] Gentry C. Fully homomorphic encryption using ideal lattices. Annual ACM Symposium on Theory of Computing. — Proceedings of the 41st annual ACM symposium on Theory of computing. 2009. — P. 169-178.

[44] Chuang I. L, N. Gershenfeld, Kubinec M. Experimental Implementation of Fast Quantum Searching. — Physical Review Letters. — 1998. — 80:15. — P. 3408–3411.

[45] Пат. № 43779 України, МПК H04L 9/08. Система передачі криптографічних ключів / Гнатюк С.О., Кінзерявий В.М., Корченко О.Г. —

№u200904239; заявл. 29.04.2009; опубл. 25.08.2009, Бюл. №16.

[46] Пат. № 2302085 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей / Молотков С., Кулик С. — № 200513476; 16.11.2005.

[47] Пат. № 2325039 РФ, H04L9/00 (2006.01). Способ кодирования и передачи криптографических ключей / Молотков С., Кулик С. — № 2006119652; 06.06.2006.

[48] Pat. № 7461323 USA, H03M 13/00 (20060101). Quantum key delivery method and communication device / Matsumoto, Wataru et al — 02.12.2008.

[49] Pat. № 7266304 USA, H04B 10/00 (20060101), H04K 1/00 (20060101). System for secure optical transmission of binary code / Duraffourg, Laurent et al — 04.09.2007.

[50] Pat. № 7178277 USA, H04K 1/00 (20060101). Quantum cryptography communication system and quantum cryptography key distributing method used in the same / Takeuchi, Takeshi et al — 20.02.2007.

[51] Pat. № 6748081 USA, H04L 9/08 (20060101), C09K 19/02 (20060101), G02F 1/13 (20060101). Quantum cryptography system for a secure transmission of random keys using a polarization setting method / Dultz, Wolfgang et al — 08.06.2004.

[52] Pat. № 6438234 USA, H04L 9/08 (20060101), H04K 001/00. Quantum cryptography device and method / Gisin, Zbinden et al — 20.08.2002.

УДК 003.26:004.056.55:621.39 (045)

Рябый М.А. Обзор современных методов квантовой и пост-квантовой криптографии

Аннотация. *Квантовый компьютер может разрушить большинство, если не все традиционные криптосистемы, используемых на практике, а именно, все системы на основе задачи факторизации целых чисел (например, RSA) или задачи дискретного логарифмирования (как традиционных, так и на эллиптических кривых Диффи-Хеллмана и DSA, а также всю криптографию, основанную на спаривание). Некоторые классические криптосхемы, базирующиеся на вычислительно-сложных задачах, сильно отличаются от указанных выше и их сложнее решить, они остаются независимыми от квантовых вычислений. В данной работе проведен обзор методов защиты информации на базе квантовых и пост-квантовых технологий. Для каждого из методов защиты информации на базе квантовых технологий приведены преимущества и недостатки. Описаны системы пост-квантовой криптографии на основе теории решеток. Результаты проведенного обзора позволяют формализовать направления дальнейших исследований пост-квантовых методов и разработки новых эффективных систем защиты информации с использованием квантовых технологий.*

Ключевые слова: *защита информации, квантовая криптография, пост-квантовая криптография, квантовый распределение ключей, квантовый компьютер, криптография на основе теории решеток.*

Ryabyy M. Review of current methods of quantum and post-quantum cryptography

Abstract. *A quantum computer can destroy most, if not all, of the traditional cryptosystems used in practice, namely, all the systems on the basis of the integer factorization problem (e. g. RSA) or the discrete logarithm problem (both traditional and elliptic curve Diffie-Hellman and DSA, and the whole cryptography based on the pairing). Some classic cryptosystems based on computationally difficult problems are very different from the above and more difficult to solve, they are independent of the quantum computation. In this paper, a review of methods of information security based on quantum and post-quantum technologies was carried out. For each of the methods of information security based on quantum technologies are the advantages and disadvantages. Describes the system of post-quantum cryptography based on lattice theory. The results of the survey allow to formalize the direction of future research of post-quantum methods and development of new effective information security systems using quantum technologies.*

Key words: *information security, quantum cryptography, post-quantum cryptography, quantum key distribution, quantum computers, cryptography based on lattice theory.*

Отримано *8 жовтня 2014 року*, затверджено редколегією *28 жовтня 2014 року*