УДК 004.056

Ю. І. Горбенко, Р. С. Ганзя
Приватне акціонерне товариство
“Інститут інформаційних технологій”

АНАЛІЗ ШЛЯХІВ РОЗВИТКУ КРИПТОГРАФІЇ ПІСЛЯ ПОЯВИ КВАНТОВИХ КОМП’ЮТЕРІВ

Наведено оцінки стійкості сучасних популярних асиметричних та симетричних криптосистем проти квантового криптоаналізу на основі алгоритмів Шора та Гровера, а також проти класичних алгоритмів криптоаналізу. Окреслено основні напрями розвитку постквантової криптографії та проведено оцінку можливостей застосування на практиці криптосистем, що є стійкими, на цей момент, до квантового криптоаналізу.

Ключові слова: алгоритм Шора, алгоритм Гровера, постквантова криптографія, RSA, ECC, NTRU.

CRYPTOGRAPHY DEVELOPMENT WAYS ANALYSIS AFTER QUANTUM COMPUTERS ORIGIN

The article presents the evaluation of the resistance of modern popular asymmetric and symmetric cryptosystems against cryptanalysis based on quantum Shor’s algorithm and Grover’s algorithm and against classical algorithms of cryptanalysis. There we present basic directions of postquantum cryptography and possibilities of the practical application of cryptosystems that are stable at the moment against the quantum cryptanalysis.

Key words: Shor’s algorithm, Grover's algorithm, postquantum cryptography, RSA, ECC, NTRU.

Вступ

Безпека сучасних інформаційних систем та технологій ґрунтується на стійкості криптографічних перетворень, які вони використовують для криптографічної обробки інформації. Криптографічна стійкість базується на складності розв’язання певних математичних задач (факторизації великого цілого числа, розв’язку дискретного логарифма тощо), для таких задач характерна субекспоненційна або експоненційна складність розв’язання на сучасних (класичних) комп’ютерах. Проте, використовуючи квантові алгоритми Шора [1] та Гровера [2], певні математичні задачі можна розв’язувати навіть з поліноміальною складністю. Ідеї використання потужностей квантового середовища висунули Пауль і Фейнман [3]. Важливим стало розроблення у 1992 р. Дойтчем [4] та іншими першого квантового алгоритму, можливості якого значно перевищували можливості звичайних комп’ютерів. У випадку появи квантового комп’ютера, на якому може бути запущений квантовий алгоритм криптоаналізу Шора або алгоритм пошуку в неупорядкованій базі даних Гровера [2], можуть виникнути великі загрози у інформаційній сфері відносно забезпечення криптографічної стійкості як для асиметричних криптоперетворень, так і для певних симетричних. Важливим є не тільки сам факт побудови такого комп’ютера, а й технічні характеристики, якими володітиме квантовий комп’ютер.

Ураховуючи небезпеку, яку становлять квантові алгоритми, що можна застосувати для криптоаналізу сучасних криптосистем, за останні роки вже було запропоновано певні класи криптосистем, що будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та

Гровера [5–8]. Крім цього, активні дослідження ведуться у напрямі квантових протоколів та квантових генераторів випадкових послідовностей.

Аналіз досліджень та публікацій

У роботі [1] наведено опис квантового алгоритму Шора для знаходження періоду функції, який можна використати для факторизації цілих чисел та розв'язання дискретного логарифмічного рівняння. Детальний аналіз можливостей алгоритму Шора наведено в роботі [9]. В роботі [2] Гровер навів квантовий алгоритм пошуку в неупорядкованій базі даних, аналіз можливостей використання алгоритму Гровера для проведення криптоаналізу сучасних криптосистем подано в роботі [10].

У роботах [9, 10] наведено наші оцінки стійкості сучасних асиметричних та симетричних криптосистем проти квантового криптоаналізу. В роботі [10] описано можливості використання алгоритму Гровера для криптоаналізу криптосистеми типу NTRU [6] та наведено оцінки складності криптоаналізу класичними та квантовими методами цієї системи.

Після того, як Шор у 1994 р. запропонував поліноміальний алгоритм знаходження періоду функції, багато криптографів та математиків почали працювати у напрямі постквантової криптографії, тобто криптографії, яка існуватиме після появи квантового комп'ютера [5]. Вже існують певні класи криптосистем, які за структурою будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та Гровера. Такі криптосистеми, як правило, презентуються та обговорюються на щорічній конференції PQCrypto з 2006 р. [7].

Постановка завдання

Основне завдання цієї статті – аналіз можливостей застосування сучасних криптосистем після появи квантових комп'ютерів, на яких можна застосувати квантові алгоритми Шора та Гровера, а також аналіз відомих класів криптосистем постквантової криптографії та перспективи їх розвитку в Україні.

1. Порівняння класичного та квантового алгоритмів криптоаналізу сучасних асиметричних криптосистем

Квантові алгоритми Шора та Гровера для проведення криптоаналізу потребують квантового комп'ютера, в якому поведінка системи кубітів визначатиметься законами квантової механіки, а також достатньо великої (на поточний момент) кількості кубітів. Тривалий час до створення квантового комп'ютера ставились достатньо скептично, але у 2007 р. канадська компанія D-Wave презентувала свій 16-кубітний квантовий комп'ютер, а вже у 2013 р. вона продала комп'ютер із 512 кубітами Google та NASA [11]. Тобто за достатньо невеликий проміжок часу колектив дослідників компанії D-Wave досяг значних успіхів у збільшенні кількості кубітів на процесорі квантового комп'ютера.

Створенням квантового комп'ютера займаються багато наукових колективів, серед них такі як Каліфорнійський технологічний інститут, IBM, D-Wave Systems, Російський квантовий центр та Національний дослідницький технологічний інститут "МІСіС". Кожний з колективів вже досяг значних успіхів у напрямі побудови такого комп'ютера, але найвагоміші результати все ще у D-Wave, проте, як показує аналіз, комп'ютер D-Wave не підходить для реалізації алгоритмів квантового криптоаналізу, тому що на ньому неможливо реалізувати алгоритми, які використовують квантові вентилі. Тобто вважається, що ні алгоритм Шора, ні алгоритм Гровера на ньому не можуть бути реалізованими [9,10]. Це пов'язано з тим, що для обчислень використовується зовсім інший принцип – так звані адіабатичні квантові обчислення. Вказане значно обмежує його можливості, але дозволяє не турбуватися про декогеренції та інші проблеми, що характерні для звичайних квантових обчислювачів.

Важливим є факт, що став відомим на початку 2014 року, на основі документів [12], що надав колишній підрядник Агентства національної безпеки США (АНБ) Едвард Сноуден. Документи свідчать про те, що АНБ запустило дослідницьку програму, на яку виділено $ 79,7 млн., під назвою "Проникнення до важких цілей" з метою розроблення квантового комп'ютера, здатного зламати шифрування, що є уразливим для квантових комп'ютерів.

Дуже поширені сьогодні й часто застосовуються алгоритми асиметричного перетворення в кільці, в групі та в групі точок еліптичної кривої, прикладами таких криптосистем є RSA, DSA, ECC. Більшість атак на такі криптосистеми спрямовані на знаходження особистого ключа. Так, для криптосистеми RSA стійкість проти такої атаки базується на складності факторизації модуля перетворення N. Усі відомі нині класичні алгоритми факторизації мають або експоненційну, або субекспоненційну складність. Вважається, що найкращим з погляду мінімізації складності факторизації є алгоритм загального решета числового поля або його модифікації. Часова складність таких алгоритмів оцінюється як субекспоненційна, наприклад, у вигляді [9]:

$$O(\exp(\delta + o(1)(\ln N)^{\gamma}(\ln\ln N)^{1-\gamma})), \delta = 1.92, \gamma = 1/3. \quad (1)$$

Водночас квантовий алгоритм Шора має поліноміальну складність. Він здатен розкласти складене число на прості множники приблизно за час:

$$O(4n^3), \quad (2)$$

з використанням такої кількості кубітів:

$$O(2n), \quad (3)$$

де n – кількість бітів у розмірі модуля перетворення.

Пропозиція та оцінки складності алгоритму Шора вразили, пробудивши широкий інтерес до квантових обчислень. В алгоритмі Шора використано ефект квантового паралелізму, який запропоновано для отримання суперпозиції всіх значень функції за один крок. Після цього здійснюють квантове перетворення Фур'є функції. Подальші обчислення дають змогу визначити з великою ймовірністю період модуля перетворення, який використовується для його факторизації. Стосовно роботи алгоритму – більша його частина припадає на перетворення Фур'є, що базується на алгоритмі швидкого перетворення Фур'є [1].

Порівняльний аналіз класичного алгоритму і квантового алгоритму факторизації наведено у табл. 1.

Таблиця 1

Порівняльний аналіз класичного алгоритму і квантового факторизації (RSA)

Розмір модуля, бітів	Кількість необхідних кубітів	Складність квантового алгоритму, квантових гейтів	Складність класичного алгоритму, оп. множення
512	1024	$0.54\cdot10^{9}$	$1.6\cdot10^{19}$
768	1536	$1.8\cdot10^{9}$	$9.9\cdot10^{22}$
1024	2048	$4.3\cdot10^{9}$	$1.2\cdot10^{26}$
2048	4096	$34\cdot10^{9}$	$1.35\cdot10^{35}$
3072	6144	$12\cdot10^{10}$	$5\cdot10^{41}$
15360	30720	$1.5\cdot10^{13}$	$9.2\cdot10^{80}$

Аналіз даних табл. 1 показує, що для зламу RSA криптосистеми з розміром модуля у 15360 бітів (розмір головного сертифіката відкритого ключа США) необхідно лише $1.5\cdot10^{13}$ операцій на квантовому комп’ютері, тоді як класична обчислювальна система повинна виконати близько 10^{80} операцій. Тобто RSA система буде зламана за поліноміальний час. Крім того, як випливає із табл. 1, навіть істотне збільшення модуля не врятовує RSA криптосистему від її злому.

Проведений аналіз показує [9], що алгоритм Шора дискретного логарифмування в групі точок еліптичної кривої та в скінченному полі має однакові кроки, єдина відмінність – це представлення точок еліптичної кривої та елементів поля. Нині вважається, що задачі дискретного логарифмування у групі точок еліптичних кривих найефективніше можна розв’язати з використанням ρ- та λ-методів Полларда. Для них складність можна оцінити як:

$$O(\sqrt{q}), \quad (4)$$

де q – кількість точок еліптичної кривої.

Водночас квантовий алгоритм Шора у загальному випадку здатен розв'язати логарифмічне рівняння приблизно за такий час:

$$O(360n^3), \tag{5}$$

та з використанням такої кількості кубітів:

$$O(7n + 4\log_2 n + 10), \tag{6}$$

де n – розмір базової точки [9].

Детальний порівняльний аналіз класичного алгоритму та квантового алгоритму Шора для розв'язку дискретного логарифма в групі точок еліптичної кривої наведено у табл. 2.

Таблиця 2

Порівняльний аналіз складності класичного і квантового алгоритмів дискретного логарифмування у групі точок еліптичної кривої (ECC)

Розмір порядку базової точки, бітів	Кількість необхідних кубітів	Складність квантового алгоритму	Складність класичного алгоритму
110	808	$0.5\cdot10^{9}$	$3.6\cdot10^{16}$
163	1210	$1.6\cdot10^{9}$	$3.4\cdot10^{24}$
224	1610	$4\cdot10^{9}$	$5.2\cdot10^{33}$
256	1834	$6\cdot10^{9}$	$3.4\cdot10^{38}$
509	3610	$4.7\cdot10^{10}$	$4\cdot10^{76}$
571	4016	$6.7\cdot10^{10}$	$8.8\cdot10^{85}$
1024	7218	$3.8\cdot10^{11}$	$1.3\cdot10^{154}$
2048	14390	$3.1\cdot10^{12}$	$1.8\cdot10^{308}$

Із даних табл. 2 видно, що навіть збільшення розміру порядку базової точки під час криптоаналізу з використанням квантового алгоритму суттєво не збільшує криптографічну стійкість. Також видно, що у разі збільшення модуля складність дискретного логарифмування класичними методами в групі точок еліптичної кривої зі збільшенням порядку базової точки збільшується суттєво. Але для квантового алгоритму проблемою є велика кількість кубітів, яка необхідна для проведення квантової атаки. Причому це залишається проблемним навіть в умовах появи квантових комп'ютерів, що здатні виконати алгоритм Шора. Вважається, що така велика кількість кубітів тривалий час буде недоступною. Саме на цьому і може базуватися стійкість таких систем, але це є лише тимчасовим вирішенням проблеми.

Необхідно зауважити, що для забезпечення криптографічної стійкості перетворень у групі точок еліптичних кривих, бо саме таке перетворення використовується в національному стандарті ДСТУ-4145, в перспективі необхідно збільшувати розміри загальних параметрів з порядком базової точки навіть до 1024 бітів.

Можливості протидії квантовому криптоаналізу

Основним напрямом протидії квантовим алгоритмам криптоаналізу є винайдення нових класів криптосистем, стійкість яких не ґрунтується на таких математичних проблемах, як складність факторизації цілого числа чи розв'язку дискретного логарифма. Напрям таких досліджень названо терміном "постквантова криптографія", тобто криптографія, яка буде стійкою навіть після появи квантового комп'ютера, що матиме велику кількість кубітів для своєї роботи. Цей напрям робіт популяризувався після 2006 р., саме тоді проведено першу конференцію за цією тематикою (PostQuantumCrypto 2006) [7]. Така конференція проводиться щорічно, щоб обговорити найкращі здобутки за рік у напрямі постквантової криптографії.

Що стосується симетричних криптосистем, то більшість сучасних симетричних шифрів та геш-функцій захищені від квантових комп'ютерів. Квантовий алгоритм Гровера може прискорити криптоаналіз таких криптосистем, але йому можна протидіяти збільшенням розміру ключа чи блока повідомлення [10]. Короткий аналіз можливостей алгоритму Гровера щодо криптоаналізу симетричних криптосистем наведено нижче.

Отже, враховуючи останні досягнення у напрямі постквантової криптографії, можна виділити такі класи криптосистем, що будуть стійкими до квантового криптоаналізу [5]:

1. Криптографія на основі решіток.
2. Мультиваріативна криптографія.
3. Криптографія на основі геш-функцій.
4. Криптографія на основі кодів.
5. Криптографія ізогінеї суперсингулярних еліптичних кривих.
6. Симетрична криптографія.

Аналіз можливостей застосування криптографії на основі решіток у постквантовому світі

Криптографія на основі решіток є новітнім класом альтернативних схем відкритого ключа і сьогодні являє собою активну область для досліджень. Є кілька складних проблем, які можна використати, щоб побудувати криптосистеми на базі решіток, найпопулярнішою є проблема знаходження найкоротшого вектора.

Цей напрям охоплює такі криптографічні системи, як NTRU [6] та GGH. Згідно з Micciancio і Регева [5], криптографію на основі решіток можна розділити на дві категорії: практичні криптосистеми, такі як NTRU, які не володіють доказами безпеки таких схем, і теоретичні, такі як матриці на основі навчання з помилками (Learning with Errors, LWE), які пропонують сильні докази безпеки, але використовують ключі, занадто великі для загального використання. З 2008 р. ведуться дослідження із об’єднання цих двох категорій, проте все ще не вдалося це зробити і створити новий клас криптографічних систем на основі решіток, які б діяли ефективно, як NTRU, і були б доказово стійкими, як LWE.

Схема шифрування і розшифрування NTRU є дуже швидкою. Вони складаються з однієї та двох дискретних згорток, відповідно. Операндами є поліноми над кільцем цілих чисел. Степінь полінома зазвичай нижчий за 800, і ціле кільце Z_q зазвичай задається простим числом з довжиною 8–10 бітів. Основна операція в генерації ключів – це поліноміальна інверсія, яка досягається за рахунок розширених евклідових алгоритмів [6].

Отже, криптографічні конструкції на основі решіток мають великі перспективи для використання в інформаційній сфері. Так, криптосистема NTRU вже стандартизована (стандарт IEEE 1363.1) і використовується для надання послуги конфіденційності. Для України є важливим розвиток цього напряму, як показують наші дослідження [10], хоча й існують квантові атаки на криптосистему типу NTRU, які є значно ефективнішими, ніж відомі класичні атаки, проте вони вимагають все одно субекспоненційної кількості квантових гейтів для реалізації на реальні криптосистеми.

Аналіз можливостей застосування криптографії на основі геш-функцій у постквантовому світі

Ядром такого класу криптосистем є те, що звичайні геш-функції використовують як базову операцію для генерації цифрових підписів, як правило, за допомогою напрямленого дерева графів. Таку ідею висунув в 1979 р. Лампорт [5, 8], він запропонував схему одноразового підпису. Ідею Лампорта покращив Вінтерніц з метою забезпечення ефективнішого підписання великого об’єму даних. У 1989 р. Меркле опублікував схему цифрового підпису на основі дерева геш-функцій для підвищення кількості разових підписів, що запропонував Лампорт. Таку схему назвали схемою підпису Меркле (MSS), вона дозволяє збільшити кількість підписів з використанням однієї зв’язки особистого та відкритого ключа, оскільки в двійковій системі геш-дерево сильно зменшується необхідний обсяг пам'яті. Перевагою MSS є доказ її безпеки, що покладається тільки на безпеку використаної геш-функції. Недоліком такої схеми є обмежена кількість підписів, які можна виготовити з однією парою ключів. Цю проблему вирішено побудовою декількох рівнів геш-дерев

Меркле. Схеми підпису на основі геш-функцій адаптуються до різних сценаріїв застосування. Їх продуктивність, розміри ключів і розміри підпису залежать від того, яку геш-функцію покладено в основу, максимальну кількість підписів та інші фактори можна регулювати для кожного випадку застосування криптосистеми окремо.

MSS має надзвичайно короткий відкритий ключ (довжина є виходом геш-функції, покладеної в основу), порівняно велику довжину підпису, проте в цій схемі генерація ключів є обчислювально дорогою. Незважаючи на це, особистий ключ є доволі великим, але його не обов'язково зберігати весь, його частина може бути згенерована "на льоту". Високий ступінь свободи для застосування такої криптосистеми надає вибір геш-функції, що буде використана для створення підпису. Можливі алгоритми, такі як SHA-1 або SHA-2 або будь-який алгоритм блочного шифрування. Отже, є багато варіантів конструкції криптосистеми на базі геш-функцій.

Попри такі недоліки цього класу криптосистем, як обмежена кількість застосувань для одного набору ключів або побудова декількох рівнів дерев геш-функцій, є і переваги, а саме свобода вибору геш-функцій, які становитимуть ядро такої криптосистеми, а також значна швидкодія такої криптосистеми і невеликий розмір ключових даних. Стійкість такої криптосистеми залежить від того, яка геш-функція використовується, адже в Україні незабаром з'явиться національний стандарт геш-функції з розміром вихідних даних до 512 бітів. Такий напрям розвитку постквантових криптосистем є надзвичайно цікавим і для застосування в інформаційних системах на національному рівні, важливим аспектом є те, що такі криптосистеми будуть стійкими до квантового криптоаналізу [8].

Аналіз можливостей застосування симетричної криптографії у постквантовому світі

Метод Гровера [2] розв'язує задачу, яку можна сформулювати так: нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент з деякою властивістю (яка легко перевіряється) і потрібно знайти цей елемент. Так, алгоритм Гровера може бути застосований для криптоаналізу геш-функцій чи симетричних шифрів. З використанням алгоритму Гровера можна знайти секретний ключ симетричного шифрування за час $\sqrt{K}$, де K – розмір ключа. Детальний опис стійкості симетричних систем проти квантового криптоаналізу наведено в табл. 3 та в роботі [10].

Таблиця 3

Стійкість популярних симетричних шифрів проти квантового криптоаналізу в разі атаки на ключ та на блок повідомлення

№ з/п	Шифр	Розмір блока/ключа, біт	Кількість необхідної пам'яті для атаки на блок повідомлення/ключ, кубіт	Стійкість у разі атаки на	
				блок повідомлення, квантових гейтів	ключ, квантових гейтів
1	AES-128	128/128	128/128	$2^{64}(10^{19,2})$	$2^{64}(10^{19,2})$
2	AES-256	128/256	128/256	$2^{64}(10^{19,2})$	$2^{128}(10^{38,4})$
3	DES	64/56	64/56	$2^{32}(10^{9,6})$	$2^{28}(10^{8,4})$
4	TDES	64/168	64/168	$2^{32}(10^{9,6})$	$2^{134}(10^{40,2})$
5	ГОСТ-28147	64/256	64/256	$2^{32}(10^{9,6})$	$2^{128}(10^{38,4})$
6	Калина-128	128/128	128/128	$2^{64}(10^{19,2})$	$2^{64}(10^{19,2})$
7	Калина-256	256/256	256/256	$2^{128}(10^{38,4})$	$2^{128}(10^{38,4})$
8	Калина-512	512/512	512/512	$2^{256}(10^{76,8})$	$2^{256}(10^{76,8})$
9	Blowfish	64/448	64/448	$2^{32}(10^{9,6})$	$2^{224}(10^{67,2})$

З табл. 3 чудово видно, що стійкість симетричних шифрів в разі атаки з використанням квантового алгоритму суттєво зменшується. Це означає, що DES може бути повністю скомпрометований і неможливо буде вважати його стійким, його стійкість дорівнюватиме 2^{28}.

Навіть при AES бажано використовувати ключ 256 бітів. Тобто загалом алгоритм Гровера, хоча і зменшує стійкість сучасних симетричних криптосистем, але все одно потребує субекспоненційної кількості квантових гейтів, на відміну від алгоритму Шора.

Отже, бажано використовувати симетричні криптосистеми з розмірами загальносистемних параметрів понад 256 бітів, в Україні незабаром буде прийнятий стандарт симетричного шифрування з можливими розмірами загальносистемних параметрів (блока повідомлення і ключа) 512 бітів і таку криптосистему можна вважати стійкою до квантового криптоаналізу на основі алгоритму Гровера.

Аналіз можливостей застосування інших класів постквантової криптографії

У 1978 р. Мак-Еліс запропонував схему шифрування з відкритим ключем на основі кодів, що виправляють помилки [5]. Ця криптосистема зараз є однією з найбільш вивчених криптосистем з відкритим ключем. Криптосистема Мак-Еліса основана на ідеї того, що існують ефективні декодери для деяких кодів, як, наприклад, коди Гоппа, але не для загальних лінійних кодів, для яких декодування є NP-важкою задачею. Після цього запропоновано ще деякі криптосистеми, що базуються на такій ідеї, наприклад, криптосистема Niederreiter або деякі інші схеми підпису на основі кодів.

Основною операцією такої схеми з використанням кодів є множення матриці-вектора, що робить його дуже ефективним (насправді швидше, ніж більшість сучасних асиметричних схем). Основна операція під час розшифрування – це декодування кодів Гоппа над полем GF (2^m), що, як правило, використовують розширений алгоритм Евкліда, який є ефективним для параметрів, що використовуються у схемі Мак-Еліса. Ключові розміри для безпечних наборів параметрів змінюються від сотень кілобайт до мегабайт для особистого ключа. Генерація ключів залучає операцію інверсії матриці, яка також є ефективною. Отже, з практичного погляду, криптосистема на основі кодів має такі особливості: швидке шифрування / розшифрування, великий рівень безпеки, але є і недоліки: великі розміри ключів, накладні шифрування, дорогі з обчислювального погляду операції виготовлення підпису.

Інший клас криптосистем, що можуть використовуватися у постквантовому світі, – це криптосистеми, основані на проблемі розв’язання багатовимірних квадратних рівнянь (MQ-проблема) над кінцевими полями. Розв’язання MQ рівнянь, як відомо, є NP-складною задачею і різні схеми MQ намагаються наблизитися до загального випадку. Вже запропоновано схеми підпису та шифрування, основані на проблемі розв’язання багатовимірних квадратних рівнянь, але тільки схеми підпису є стійкими до криптоаналізу.

Криптографія, основана на ізогінеї, є цікавою альтернативою наведеним вище напрямам постквантової криптографії [13]. Це пояснюється тим, що вона базується на природній обчислювальній проблемі теорії чисел, а саме на проблемі підрахунку ізогінезису між еліптичними кривими. Ці системи можна зарахувати до одного з напрямів постквантової криптографії, вони грунтуються на теоретико-числовому припущенні. Оскільки національний стандарт вироблення та перевірки цифрового підпису базується на еліптичних кривих, то такий напрям є надзвичайно важливим і перспективним для використання в Україні.

Якщо коротко охарактеризувати постквантові криптосистеми, то криптосистеми на основі решіток сьогодні призначені більше для шифрування інформації. Схеми вироблення цифрових підписів на основі решіток менш розвинені, ніж схеми шифрування. Водночас криптосистеми на базі геш-функцій та мультиваріативні поліноми тепер більш готові для вироблення цифрових підписів, ніж для шифрування інформації, а криптосистеми на базі ізогінеї більш пов’язані з шифруванням та з протоколом автентифікації. Класично протоколи автентифікації суб’єкта пов’язують зі схемою Фіат–Шаміра, проте така схема вразлива до можливостей квантового криптоаналізу. Нещодавно запропоновано схему на основі ізогінезису еліптичних кривих, яка пропонує схему виготовлення та перевірки цифрового підпису, автентифікації та може бути

застосована у постквантовому світі [13]. Поки що важко побудувати схеми цифрового підпису, які будуть стійкими до квантового криптоаналізу, єдина відома незаперечна схема підпису, що запропонована, основана на лінійних кодах.

Порівняння класів постквантових криптосистем (крім симетричних шифрів) наведено у табл. 4.

Таблиця 4

Порівняння постквантових криптосистем

Клас криптосистеми	Вироблення / перевірка підпису	Шифрування / розшифрування	Розмір ключа	Тип даних	Основні операції
На основі решіток: NTRU загальні решітки	 Можливо Можливо	 Так Так	 <0,1 кБ ≈ 100 кБ	 Z_q $GF(2^m)$	 Згортання Множення матриць
Мультиваріативні поліноми	Так	Ні	≈ 10 кБ	$GF(2^m)$	Множення матриць, розв'язання лінійної системи рівнянь
На основі геш-функцій	Так	Ні	≈ 20 Б	Вихід геш-функції	Гешування
На основі кодів	Потребує багато обчислень	Так	≈ 100 кБ	$GF(2^m)$	Множення матриць, декодування
Ізогінезис суперсингулярних еліптичних кривих	Так	Ні (наявний протокол встановлення ключів)	<1 кБ	GF(p)	Операції на еліптичній кривій

Висновки

Наведено наші оцінки стійкості сучасних популярних асиметричних криптосистем на основі таких математичних проблем, як складність факторизації цілого числа та розв'язання дискретного логарифмічного рівняння (у полі та в групі точок еліптичної кривої) проти класичного та квантового криптоаналізу. Оцінки показують, що з використанням алгоритму Шора такі криптосистеми, як RSA, DSA, ECC та подібні до них, будуть скомпрометовані з використанням поліноміального числа квантових гейтів, хоча з використанням класичних комп'ютерів такі задачі розв'язуються з субекспоненційною чи експоненційною складністю. З використанням алгоритму Гровера можна значно зменшити складність атаки на симетричні криптосистеми (блочні шифри та геш-функції) та криптосистеми на базі решіток (NTRU), проте такий криптоаналіз потребує субекспоненційної кількості квантових гейтів.

Хоча стійкість асиметричних криптосистем є поліноміальною і збільшення розмірів загальносистемних параметрів суттєво не підвищує стійкості проти квантового криптоаналізу, проте для його проведення квантовий комп'ютер повинен мати доволі велику, на цей момент, кількість кубітів, саме на цьому може грунтуватися певний час стійкість таких криптосистем. Розміри загальносистемних параметрів криптосистеми на базі еліптичних кривих можна підвищити аж до 1024 бітів, тоді квантовий комп'ютер повинен мати 7218-кубітний процесор для зламу такої криптосистеми.

В статті проаналізовано постквантові криптосистеми, які можуть застосовуватися у випадку появи квантових комп'ютерів, здатних реалізувати квантові алгоритми Шора та Гровера. До постквантових криптосистем можна зарахувати криптосистеми на основі решіток, мультиваріативних поліномів, геш-функцій, кодів, ізогінеї суперсингулярних еліптичних кривих, а також всю симетричну криптографію. Важливим є розвиток цих класів постквантових

криптосистем і в Україні, особливо цікавими залишаються криптосистеми на базі решіток та ізогінеї суперсингулярних еліптичних кривих. Проте, як показує аналіз постквантових криптосистем, поки що не існує постквантової криптосистеми, яка б змогла замінити усі сучасні асиметричні криптосистеми. Кожна з постквантових криптосистем має певні переваги та недоліки, саме тому напрям постквантової криптографії вимагає подальшого дослідження.

1. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text] / P. W. Shor //S IAM J. Comput. – 1997. – 26 (5). – P. 1484–1509. 2. Grover L. K. A fast quantum mechanics algorithm for database search [Text] / L. K. Grover // Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. – 1996. – P. 212–219. 3. Feyman R. P. Quantum mechanical computers [Text] / R. P. Feyman // Opt. News – 1985. – February, 11. – P. 11–39. 4. Deutsch D. Rapid Solution of problems by quantum computation [Text] / Deutsch D., Jozsa R. // Proc. R. Soc. Lond. A. – 1992. – Vol. 439 (1907). – P. 553–558. 5. Bernstein, D. Post-quantum cryptography [Text] / D. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 246 p. 6. IEEE Std 1363. 1-2008. IEEE Standard Specification for Public Key Cryptographic Tehniques Based on Hard Problems over Lattice [Text]. 2009 – 04 – 10 – NY: The Institute of Electrical and Electronics Engineers, Inc. – 2009. – 69 p. 7. Main page of PQCrypto 2014 [Electronic resource] / University of waterloo, Ontario, Canada Сайт конференції PQCrypto 2014 Режим доступа: \www/ URL:– https://pqcrypto2014.uwaterloo.ca. – 21.08.2014 р. 8. Stefan Heyse. Post quantum cryptography: implementing alternative public key schemes on embedded devices: dissertation for the degree of doktor-ingenieur: 10.2013 / Stefan Heyse. – Bochum, 2013. – 235 p. – Bibliogr.: P. 205–223. 9. Горбенко Ю. І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Восточно-Европейский журнал передовых технологий. – Харків, 2014. – Том 6, №1(67). – С. 8–15. 10. Горбенко Ю. І. Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера / Ю. І. Горбенко, Р. С. Ганзя // Захист інформації: науково-практичний журнал. – К., 2014. – Том 16, №2. – С. 106–112. 11. Launching the quantum artificial intelligence lab [Electronic resource] / Блог компанії Google: Режим доступа: \www/ URL:— http://googleresearch.blogspot.ru/2013/05/launching-quantum-artificial.html. 16.05.2012 р. 12. NSA seeks to build quantum computer that could crack most types of encryption [Electronic resource] / Steven Rich and Barton Gellman, стаття в "The Washington Post": Режим доступа: \www/ URL:— http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html – 10.01.2014 р. 13. De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [Text] / L. De Feo, D. Jao, J. Plut // PQCrypto. – 2011. – 24 p.