УДК 004.056

АНАЛІЗ СТІЙКОСТІ ПОСТКВАНТОВИХ КРИПТОСИСТЕМ

Ю.І. ГОРБЕНКО, Р.С. ГАНЗЯ

В роботі наводяться оцінки стійкості популярних асиметричних криптосистем проти квантового криптоаналізу на основі алгоритму Шора, показано основні класи криптосистем, що будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та Гровера. Наводяться оцінки стійкості постквантових криптосистем проти класичного та квантового криптоаналізу.

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

ВСТУП

Безпека сучасних інформаційних систем та технологій базується на стійкості криптографічних перетворень, які вони використовують для криптографічної обробки інформації. Так з використанням алгоритму Шора [1] складність криптоаналізу таких криптосистем як RSA, DSA, ECC буде поліноміальною, хоча з використанням класичних алгоритмів криптоаналізу, відомих на сьогодні, складність атаки на такі криптосистеми є субекспоненційною або експоненційною. Використовуючи алгоритм Гровера [2] можна зменшити складність атаки на симетричні криптосистеми та деякі криптосистеми на основі фактор-кілець.

Після винайдення Шором у 1994 році поліноміального алгоритму знаходження періоду функції велика кількість криптографів та математиків почали працювати у напрямку постквантової криптографії, тобто криптографії, яка існуватиме після появи квантового комп'ютера. На сьогодні вже існують певні класи криптосистем, які за своєю 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 року. За останні роки вже було запропоновано певні класи криптосистем, що будуть стійкими до квантового криптоаналізу на основі алгоритмів Шора та Гровера [3–6].

1. ПОРІВНЯННЯ КЛАСИЧНОГО ТА КВАНТОВОГО АЛГОРИТМІВ КРИПТОАНАЛІЗУ СУЧАСНИХ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

Квантові алгоритми Шора та Гровера для проведення криптоаналізу потребують квантовий комп'ютер, у якому поведінка системи кубітів визначатиметься законами квантової механіки, а також достатньо велику (на даний момент часу) кількість кубітів. Тривалий час можливості створення квантового комп'ютера були достатньо скептичні, але у 2007 році канадська компанія D-Wave презентувала свій 16-кубітний квантовий комп'ютер, а вже у 2013 році вона продала комп'ютер із 512 кубітами Google та NASA [7]. 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 "MICiC". Сьогодні кожний з колективів досяг значних успіхів у напрямку побудови такого комп'ютера, але найбільші результати залишаються за D-Wave, проте, як показує аналіз, комп'ютер D-Wave не підходить для реалізації алгоритмів квантового криптоаналізу, тому що на ньому не можуть бути реалізовані алгоритми, які використовують квантові вентилі. Тобто вважається, що ні алгоритм Шора, ні алгоритм Гровера на ньому не можуть бути реалізованими [7, 8]. 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 [8], наданих колишнім підрядником Агентства національної безпеки США (АНБ) Едвардом Сноуденом. Документи свідчать про те, що АНБ запустило дослідницьку програму, на яку виділено $ 79,7 млн., під назвою "Проникнення до важких цілей" з метою розробки квантового комп'ютера, здатного зламати шифрування, що є уразливим для квантових комп'ютерів.

Зараз широке розповсюдження та застосування знайшли 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 направлені на знаходження особистого ключа, так для криптосистеми RSA стійкість проти такої атаки базується на складності факторизації модуля перетворення N. Усі відомі сьогодні класичні алгоритми факторизації мають або експоненційну, або субекспоненційну складність. Вважається, що найкращим з точки зору мінімізації складності факторизації – є алгоритм

загального решета числового поля, або його модифікації. Часова складність таких алгоритмів оцінюється як субекспоненційна, наприклад, у вигляді [7]:

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

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

$$O(4n^3), \tag{2}$$

з використанням такої кількості кубітів:

$$O(2n), \tag{3}$$

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 дозволяють визначити з великою ймовірністю період модуля перетворення, який використовується для його факторизації. З точки зору часу роботи алгоритму – більша його частина припадає на перетворення Фур'є, що базується на алгоритмі швидкого перетворення Фур'є [1].

Проведений аналіз показує [7], що алгоритм Шора дискретного логарифмування у групі точок еліптичної кривої та в скінченному полі має однакові кроки, єдине в чому відмінність – це представлення точок еліптичної кривої та елементів поля. Сьогодні вважають, що вирішення задач дискретного логарифмування у групі точок еліптичних кривих найбільш ефективно може бути реалізованим з використанням ρ- та λ-методів Полларда. Для них складність можна оцінити як:

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

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.

Детальний порівняльний аналіз класичного алгоритму та квантового алгоритму Шора для розв'язку дискретного логарифму в групі точок еліптичної кривої наведено у [7].Так навіть збільшення розміру порядку базової точки в ході криптоаналізу з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості. Також видно, що зі збільшенням модуля та порядку базової точки, складність дискретного логарифмування класичними методами в групі точок еліптичної кривої суттєво зростає.

Проте 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 шляхом вирішення проблеми.

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

2. МОЖЛИВОСТІ ПРОТИДІЇ КВАНТОВОМУ КРИПТОАНАЛІЗУ

Основним напрямком 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 логарифму. Напрямок 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 напрямок робіт популяризувався після 2006 року, саме тоді була проведена перша конференція за цією тематикою (PostQuantumCrypto 2006). Така конференція проводиться щорічно і збирає для обговорення найкращі здобутки за рік у напрямку 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 блоку повідомлення [8]. Стислий аналіз можливостей алгоритму Гровера, щодо криптоаналізу симетричних криптосистем, буде наведено нижче.

Отже, враховуючи останні досягнення у напрямку постквантової криптографії, можна виділити такі класи криптосистем, що будуть стійкими до квантового криптоаналізу [3]:

- Криптографія на основі решіток.
- Мультиваріативна криптографія.
- Криптографія на основі геш-функцій.
- Криптографія на основі кодів.
- Криптографія ізогінеї суперсингулярних еліптичних кривих.
- Симетрична криптографія.

3. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ КРИПТОГРАФІЇ НА ОСНОВІ РЕШІТОК У ПОСТКВАНТОВОМУ СВІТІ

Криптографія на основі решіток є новітнім класом альтернативних схем відкритого ключа і сьогодні є активною областю для досліджень. Є кілька складних проблеми, які можуть бути використані, щоб побудувати криптосистеми на базі решіток, найпопулярнішою є проблема знаходження найкоротшого вектора.

Цей напрямок включає в себе такі криптографічні системи, як NTRU 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, які є занадто великими для загального використання. З 2008 року ведуться дослідження з об'єднання цих двох категорій, проте на сьогодні ще не вдалося об'єднати ці дві категорії і створити новий клас криптографічних систем на основі решіток, які б діяли ефективно як NTRU і були б доказово стійкими як LWE.

Протягом останніх років було запропоновано низку атак на криптосистему NTRU. Найкращою відомою класичною атакою є атака «зустріч посередині», що була запропонована в Одлижко у 2003 році, з використанням ідеї цієї атаки та квантового алгоритму Гровера у 2012 році була запропонована ефективна квантова атака на NTRU «зустріч посередині», яка в подальшому була удосконалена Вангом [8]. Аналітична часова і просторова складність таких атак наведена у табл. 1.

Таблиця 1

Аналітична складність атак на NTRU

	Класична атака «зустріч посередині»	Удосконалена квантова атака «зустріч посередині»
Часова складність	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$	$O(C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor} \log C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor}) + \bar{O}(\sqrt{C_{N-\lfloor N/3 \rfloor+1}^{d-\lfloor d/3 \rfloor}})$
Просторова складність	$O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$	$O(C_{\lfloor N/3 \rfloor}^{\lfloor d/3 \rfloor})$

Детальний аналіз стійкості криптосистеми NTRU проти квантового та класичного криптоаналізу наведено у [8]. Результати досліджень показали, що хоча квантова атака і потребує менше операцій, проте вона вимагає все одно субекспоненційної кількості квантових гейтів для реалізації на реальні криптосистеми.

Отже криптографічні конструкції на основі решіток мають великі перспективи для свого 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 напрямку, враховуючи те, що ця криптосистема є стійкою до квантового криптоаналізу, має невеликі розміри загальносистемних параметрів і має великі швидкості зашифрування/розшифрування.

4. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ КРИПТОГРАФІЇ НА ОСНОВІ ГЕШ-ФУНКЦІЙ У ПОСТКВАНТОВОМУ СВІТІ

Ядром такого класу криптосистем є те, що звичайні геш-функції використовуються як базові операції для генерації цифрових підписів, як правило, за допомогою направленого дерева графів. Така ідея була запропонована в 1979 році Лампортом [3, 5], він запропонував схему одноразового підпису. Ідея Лампорта була покращена Вінтерніцом з метою забезпечення більш ефективного підписання великого обсягу даних. У 1989 році Меркле опублікував схему цифрового підпису на основі дерева геш-функцій для підвищення разових підписів, запропонованих Лампортом. Таку схему назвали схема підпису Меркле (MSS), вона дозволяє збільшити число 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 обмежене число підписів, які можна виготовити з однією парою ключів. Ця проблема була вирішена побудовою декількох рівнів геш-дерев Меркле. Схеми підпису на основі геш-функцій адаптуються до різних сценаріїв застосування. Їх продуктивність, розміри ключів і розміри підпису залежить від того, яка геш-функція лежить в основі, 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, що лежить в основі), відносно велику довжину підпису, проте в цій схемі генерація ключів є обчислювально дорогою. Незважаючи на це, особистий ключ є досить великим, але його не обов'язково зберігати весь, його частина боже бути згенерована "на льоту". Великим ступенем свободи для застосування такої криптосистеми є вибір геш-функції, що буде використана для виробки підпису. Можливі алгоритми, такі як SHA-1 або SHA-2 або будь-який алгоритм блокового шифрування. Таким чином, є багато варіантів конструкції криптосистеми на базі геш-функцій.

Оцінка стійкості таких криптосистем базується на складності криптоаналізу геш-функцій, які є ядром такої асиметричної криптосистеми. Ймовірність такої атаки складає 1/2, складність такої атаки для класичних комп'ютерів [3]:

$$O(2^{n/2}), \quad (7)$$

для квантових комп'ютерів:

$$O(2^{n/3}). \quad (8)$$

Порівняльний аналіз квантового та класичного криптоаналізу криптосистем на базі геш-функцій наведено в табл. 2.

Таблиця 2

Порівняльний аналіз стійкості криптосистем на базі геш-функцій проти класичного та квантового криптоаналізу

Вихідна довжина, біт	128	224	256	384	512
Класична атака, бітових операцій	2^{64}	2^{112}	2^{128}	2^{192}	2^{256}
Квантова атака, квантових гейтів	2^{43}	2^{75}	2^{86}	2^{128}	2^{171}

Отже стійкість такого класу криптосистем проти квантового криптоаналізу хоча і є менше, ніж проти класичного, але вона все одно має субекспоненційну складність. Отже, враховуючи існуючі недоліки такого 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 складатимуть ядро такої криптосистеми, а також велика швидкодія такої криптосистеми і невеликий розмір ключових даних. Стійкість такої криптосистеми залежить від того, яка геш-функція використовується, оскільки в Україні незабаром з'явиться національний стандарт геш-функції з розміром вихідних даних до 512 бітів, такий напрямок 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 [5].

5. АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ СИМЕТРИЧНОЇ КРИПТОГРАФІЇ У ПОСТКВАНТОВОМУ СВІТІ

Метод Гровера [2] вирішує задачу, яка може бути сформульована так: нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент, що володіє деякою властивістю (яка легко перевіряється) і потрібно знайти цей елемент. Так алгоритм Гровера може бути застосований для криптоаналізу геш-функцій чи симетричних шифрів. З використання 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 [8].

З табл. 3 чудово видно, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму суттєво зменшується. Це означає, що DES може бути повністю скомпрометований і не можливо буде вважати його стійким, його стійкість дорівнюватиме 2^{28}. Навіть при AES бажано використовувати ключ 256 бітів. Тобто в цілому алгоритм Гровера, хоча і зменшує стійкість сучасних симетричних криптосистем, але все одно потребує субекспоненційної кількості квантових гейтів на відміну від алгоритму Шора.

Таблиця 3

Порівняльний аналіз стійкості симетричних криптосистем проти квантового криптоаналізу

Шифр	Стійкість при атаці на	
	блок повідомлення, квантових гейтів	ключ, квантових гейтів
AES-128	2^{64} $(10^{19,2})$	2^{64} $(10^{19,2})$
AES-256	2^{64} $(10^{19,2})$	2^{128} $(10^{38,4})$
DES	2^{32} $(10^{9,6})$	2^{28} $(10^{8,4})$
TDES	2^{32} $(10^{9,6})$	2^{134} $(10^{40,2})$
ГОСТ-28147	2^{32} $(10^{9,6})$	2^{128} $(10^{38,4})$
Калина-128	2^{64} $(10^{19,2})$	2^{64} $(10^{19,2})$
Калина-256	2^{128} $(10^{38,4})$	2^{128} $(10^{38,4})$
Калина-512	2^{256} $(10^{76,8})$	2^{256} $(10^{76,8})$
Blowfish	2^{32} $(10^{9,6})$	2^{224} $(10^{67,2})$

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

6. 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 є однією з найбільш вивчених криптосистем з відкритим ключем на сьогодні. Криптосистема Мак-Еліса заснована 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 було запропоновано ще деякі криптосистеми, які 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 $GF(2^m)$, які, 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. Таким чином, з практичної точки зору, криптосистема на основі кодів має такі особливості: швидке шифрування / розшифрування, великий рівень безпеки, але і мають свої недоліки: великі розміри ключів, накладні шифрування, дорогі з обчислювальної точки зору операції виготовлення підпису.

На таку криптосистему запропоновано низку різних атак, основним з них є груба сила, структурна атака, декодування набору інформації (та її квантова реалізація). У роботі [4] Бернштейном запропоновано квантову атаку декодування набору інформації і показано, що вона є набагато швидшою, ніж вважалося. Так в його роботі показано, що складність класичної атаки є:

$$c^{(1+o(1))n/\log_2 n}, \quad (9)$$

а квантової:

$$c^{(1/2+o(1))n/\log_2 n}, \quad (10)$$

де

$$c = 1/(1-R)^{(1-R)}. \quad (11)$$

Коди задаються набором параметрів (n, k, t) і тоді $R = k/n$ (швидкість коду). Код з характеристиками (1024, 524, 50) був зламаний і зараз треба використовувати більші параметри, наприклад, (4096, 3556, 45).

Атака, описана Бернштейном [4], має виконати $c^{(1/2)n/\log_2 n}$ ітерацій алгоритму Гровера, а кожне застосування алгоритму Гровера потребує $O(n^3)$ операцій з кубітами, так кожна ітерація займає $n^{o(1)}$ на квантовому комп'ютері з розміром регістра $n^{o(1)}$. Складність квантової атаки криптосистеми на базі кодів з характеристиками (4096, 3556, 45) вимагає 2^{68} ітерацій, а кожна ітерація 2^{36} кубітових операцій, отже складність атаки приблизно 2^{100}, а це не є достатнім для 128-бітного рівня стійкості.

Інший клас криптосистем, що можуть використовуватися у постквантовому світі – це криптосистеми, які засновані 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. Сьогодні були запропоновані схеми підпису та шифрування, засновані на проблемі вирішення багатовимірних квадратних рівнянь, але тільки схеми підпису є стійкими до криптоаналізу.

На такий клас криптосистем запропоновано такі атаки, як пряма атака, атака погодження, атака Кіпніс-Шаміра. Проте всі ці атаки мають субекспоненційну чи експоненційну складність, квантових атак на такий клас криптосистем ще не було запропоновано, тому що алгоритм Шора чи алгоритм Гровера не підходять для реалізації квантової версії наведених вище класичних атак [3].

Криптографія, яка заснована на ізогінеї становить цікаву альтернативу наведеним вище напрямкам постквантової криптографії [6]. Це пояснюється тим, що вона базується на природній обчислювальній проблемі теорії чисел, а саме на проблемі обрахунку ізогінезису між еліптичними кривими. Ці системи можна віднести до одного з напрямків постквантової криптографії, такі системи базуються на теоретико-числовому припущенні. Враховуючи те, що національний стандарт вироблення та перевірки цифрового підпису базується на еліптичних кривих, то такий напрямок є надзвичайно важливим і перспективним для використання в Україні.

В роботі [6] наведено аналітичні показники стійкості такої криптосистеми, де показано, що складність криптоаналізу такої криптосистеми з використанням класичних комп'ютерів складає:

$$O(\sqrt[4]{p}), \quad (12)$$

для квантових комп'ютерів:

$$O(\sqrt[6]{p}). \quad (13)$$

Порівняльний аналіз квантового та класичного криптоаналізу криптосистем на базі ізогінеї еліптичних кривих в табл. 4.

Таблиця 4

Порівняльний аналіз стійкості на базі ізогінеї еліптичних кривих проти класичного та квантового криптоаналізу

Розмір поля $GF(p)$, біт	512	768	1024	2048
Класична атака, бітових операцій	$3\cdot10^{38}$	$6\cdot10^{57}$	10^{77}	10^{154}
Квантова атака, квантових гейтів	$5\cdot10^{25}$	$3\cdot10^{38}$	$2\cdot10^{51}$	$5\cdot10^{102}$

Отже криптосистеми на базі ізогінеї еліптичних кривих мають велику стійкість як проти квантового, так і проти класичного криптоаналізу, при цьому розміри поля мають невеликі розміри.

Якщо стисло охарактеризувати постквантові криптосистеми, то криптосистеми на базі решіток, на сьогодні, призначені більше для шифрування інформації, так схеми вироблення цифрових підписів на основі решіток є менш розвинуті, ніж схеми шифрування. Водночас криптосистеми на базі геш-функцій та мультиваріативні поліноми більш готові, на сьогодні, для вироблення цифрових підписів, ніж для шифрування інформації. Криптосистеми на базі ізогінеї зараз більше пов'язані з шифруванням та з протоколом автентифікації. Класично протоколи автентифікації суб'єкта пов'язується зі схемою Фіат-Шаміра, проте така схема є уразливою до можливостей квантового криптоаналізу. Нещодавно було запропоновано схему на основі ізогінезису еліптичних кривих, яка пропонує схему виготовлення та перевірки цифрового підпису, автентифікації та може бути застосована у постквантовому світі [6]. Сьогоді важко побуду-

вати схеми цифрового підпису, які будуть стійкими до квантового криптоаналізу, єдина відома незаперечна схема підпису, що була запропонована, заснована на лінійних кодах.

Порівняння класів постквантових криптосистем (крім симетричних шифрів) наводиться у табл. 5.

ВИСНОВКИ

У статті наведено наші оцінки стійкості сучасних популярних асиметричних криптосистем на основі таких математичних проблем як складність факторизації цілого числа та вирішення дискретного логарифмічного рівняння (в полі та у 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 стійкість асиметричних криптосистем є поліноміальною і збільшення розмірів загальносистемних параметрів не дає суттєвого підвищення стійкості проти квантового криптоаналізу, проте для його проведення квантовий комп'ютер повинен мати доволі велику, на сьогодні момент, кількість кубітів, саме на цьому може ґрунтуватися певний час стійкість таких криптосистем. Розміри загальносистемних параметрів криптосистеми на базі еліптичних кривих можна підняти аж до 1024 біт, тоді квантовий комп'ютер повинен мати 7218-кубітний процесор для зламу такої криптосистеми.

У статті проведено аналіз постквантових криптосистем, які можуть застосовуватися у випадку появи квантових комп'ютерів, що можуть реалізувати квантові алгоритми Шора та Гровера. Проведений аналіз таких криптосистем показав, що з використанням алгоритму Гровера можна значно зменшити складність атаки на симетричні криптосистеми (блокові шифри та геш-функції), криптосистеми на базі решіток (NTRU), криптосистеми на базі геш-функцій, кодів та ізогінеї еліптичних кривих, проте такий криптоаналіз потребує субекспоненційної кількості квантових гейтів.

Література

[1] Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / P. W. Shor //SIAM J. Comput. – 1997. – 26 (5). –P. 1484–1509.

[2] Grover, L. K. A fast quantum mechanics algorithm for database search / L. K. Grover. // – Proceeding of the 28th ACM Symposium on Theory of Computation, New York: ACM Press. – 1996. – P. 212–219.

[3] Bernstein, D. Post-quantum cryptography / D. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 246 p.

[4] Bernstein, D. Grover vs. McEliece. Pages / D. Bernstein // Proceedings of PQCrypto 2010, Post-quantum cryptography: third international workshop proceeding. – Springer. – 2010. – P. 73–80.

[5] 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.

[6] De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies / L. De Feo, D. Jao, J. Plut // PQCrypto. – 2011. – 24 p.

[7] Горбенко, Ю.І. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю.І. Горбенко, Р.С. Ганзя // Харків: «Восточно-Европейский журнал передовых технологий». – 2014. – Том 6. № 1 (67). – 8–15 с.

[8] Горбенко Ю.І. Аналіз стійкості популярних криптоситем проти квантового криптоаналізу на основі алгоритму Гровера / Ю.І.Горбенко, Р.С.Ганзя // Київ: Захист інформації: Науково-практичний журнал,2014. – Том 16, № 2. – С. 106–112.

Надійшла до редколегії 17.06.2014

Горбенко Юрій Іванович, фото та відомості про автора див. на стор. 251.

Ганзя Роман Сергійович, випускник кафедри безпеки інформаційних технологій ХНУРЕ. Наукові інтереси: дослідження стійкості асиметричних криптосистем.

Таблиця 5

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	 Zq GF(2m)	 Згортання Множення матриць
Мультиваріативні поліноми	Так	Ні	≈10 кБ	GF(2m)	Множення матриць, рішення 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(2m)	Множення матриць, декодування
Ізогінезис суперсингулярних еліптичних кривих	Так	Ні (присутній протокол встановлення ключів)	<1 кБ	GF(p)	Операції на еліптичній кривій

УДК 004.056

Анализ стойкости постквантовых криптосистем / Ю.И.Горбенко, Р.С. Ганзя // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 268–274.

В работе приводятся оценки стойкости популярных асимметричных криптосистем против квантового криптоанализа на основе алгоритма Шора, показаны основные классы криптосистем, которые будут стойкими к квантовому криптоанализу на основе алгоритмов Шора и Гровера. Приводятся оценки стойкости постквантовых криптосистем против классического и квантового криптоанализа.

Ключевые слова: постквантовая криптография, алгоритм Шора, алгоритм Гровера, NTRU.

Табл.: 5. Библиогр.: 10 назв.

UDC 004.056

Analyzing resistance of postquantum cryptosystems / Yu.I. Gorbenko, R.S. Hanzia // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 268–274.

This paper presents estimations of resistance of popular asymmetric cryptosystems against quantum cryptanalysis based on Shor's algorithm, the basic classes of cryptosystems are shown that are resistant to quantum cryptanalysis on the bases of Shor's and Grover's algorithms. Estimations of resistance of postquantum cryptosystems against classical and quantum cryptanalyses are provided.

Keywords: postquantum cryptography, Shor's algorithm, Grover's algorithm, NTRU.

Tab.: 05. Ref.: 10 items.