2. Антипов, И. Е. Применение теории игр для защиты беспроводных wi-fi сетей [Текст] / И. Е. Антипов, Т. А. Ященко, В. С. Вовченко. // Радиотехника: Всеукр. межвед. научн.-техн. сб. 2013 Вып. 173. С. 104-107.
3. TamoGraph® Site Survey [Электронный ресурс]. Режим доступа: http:// http://www.tamos.com.
4. AirMagnet Planner [Электронный ресурс]. Режим доступа: http:// http://www.keenansystems.com.
5. Network simulation [Электронный ресурс]. Режим доступа: http:// http:// http://en.academic.ru.
6. SimulationTools.bib [Электронный ресурс]. Режим доступа: http:// http:// http:// http://www.idsia.ch.
7. Пролетарский, А. В. Беспроводные сети Wi-Fi [Текст] / А.В. Пролетарский, И. В. Баскаков, Д. Н. Чирков. – БИНОМ. Лаборатория знаний, 2007. – 178 с.
8. Джим Гейер. Беспроводные сети. Fi [Текст] / Джим Гейер. – М.: Издательский дом «Вильямс», 2005. – 192 с.
9. Kaspersky Security Bulletin. Развитие угроз в 2008 году [электронный ресурс] Режим доступа: http:// www.securelist.com
10. Шаньгин, В. Ф. Информационная безопасность компьютерных сетей и систем [Текст] / В. Ф. Шаньгин. – М.: ИД «ФЩРУМ» - ИНФРА-М, 2008. – 416 с.

УДК 004.056

# АНАЛІЗ МОЖЛИВОСТЕЙ КВАНТОВИХ КОМП'ЮТЕРІВ ТА КВАНТОВИХ ОБЧИСЛЕНЬ ДЛЯ КРИПТОАНАЛІЗУ СУЧАСНИХ КРИПТОСИСТЕМ

**Ю. І. Горбенко**
Кандидат технічних наук, старший науковий співробітник*
Лауреат державної премії в галузі науки та техніки 2012 р.
E-mail: GorbenkoU@iit.com.ua
**Р. С. Ганзя**
Інженер*
E-mail: roman.ganzya@gmail.com
*Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
пр. Леніна, 16, м. Харків, Україна, 61166

***На основі використання доступних джерел наводиться огляд та аналіз сучасних світових досягнень в області квантових обчислень та побудови квантового комп'ютера. Проводиться аналіз загроз безпеки відносно симетричних та асиметричних криптосистем у разі застосування методів квантового криптоаналізу. Наводяться оцінки просторових та часових складностей, яких потрібно досягати для успішного здійснення квантового криптоаналізу***

***Ключові слова: алгоритм Гровера, алгоритм Шора, квантовий комп'ютер, квантовий криптоаналіз***

***На основе использования доступных источников приводится обзор и анализ современных мировых достижений в области квантовых вычислений и построения квантового компьютера. Проводится анализ угроз безопасности относительно симметричных и асимметричных криптосистем в случае применения методов квантового криптоанализа. Приводятся оценки пространственных и временных сложностей, которые нужно достигать для успешного осуществления квантового криптоанализа***

***Ключевые слова: алгоритм Гровера, алгоритм Шора, квантовый компьютер, квантовый криптоанализ***

## 1. Вступ

Ще в 60 – роках Гордон Мур [1] сформулював експериментально доведене ним твердження, згідно якого в напівпровідникових мікросхемах здійснюється практично щорічне подвоєння щільності транзисторів, тобто по суті зменшення розмірів елементів в два рази. Наведене твердження отримало назву закону Мура і справджується вже майже протягом 50 років. На сьогодні розмір елементів транзистора (і, відповідно, розмір області, в якій зберігається одиниця інформації – біт) становить нанометри. У зв'язку з цим виникає питання про принципові обмеження на розміри, швидкодію та теплообмін між елементами комп'ютерних схем при їх зменшенні. На думку фізика Р. Фейнмана "закони фізики не заперечують зменшення розмірів комп'ютера до тих пір, доки біти не досягнуть розмірів окремих атомів і закони квантової механіки не стануть

домінуючими" [1]. У зв'язку зі вказаним, вже на протязі багатьох років дискусійним стало питання - чи можливо створити комп'ютер, в якому поведінка системи бітів буде визначатись законами квантової механіки.

В подальшому Паулем і Фейнманом були висунуті ідеї про використання обчислювальної потужності квантового середовища [2]. Важливим стало розроблення у 1992 році Дойтчем та іншими [3] першого квантового алгоритму, можливості якого значно перевищувала можливості звичайних (електронних) комп'ютерів.

Зважаючи на проблеми та необхідність розв'язання задач криптоаналізу, вчені особливу увагу приділили вивченню можливостей розв'язання задач криптоаналізу з використанням квантових комп'ютерів та, в першу чергу, розроблення відповідних алгоритмів для квантових комп'ютерів. Внаслідок таких досліджень у 1994 році Шором [4] були розроблені перші квантові алгоритми - факторизації та дискретного логарифмування в скінченному полі, які призначались для реалізації на квантовому комп'ютерові. Пізніше Гровером [5] було запропоновано квантовий алгоритм пошуку ключів. З цих пір почала приділятися велика увага дослідженням у квантовій сфері. Нині, незважаючи на особливу складність практичного розроблення «істинно квантового» комп'ютера [6], в цьому напрямку ведуться інтенсивні дослідження і отримано ряд важливих результатів. В першу чергу необхідно відмітити роботи математиків з розроблення методів та алгоритмів криптоаналізу [4].

## 2. Постановка проблеми

Досягнення фізики останніх років (бозе-ейнштейнівська конденсація атомів газу [7], квантовий ефект Хола, штучні періодичні структури – квантові точки, колодязі, тощо), а також розвиток лазерних та оптоволоконних технологій дали надію на можливість реалізації найближчим часом квантового комп'ютера. Такі реалізації в початковому стані вже з'являються [6, 8, 9]. Так, за створення проривних технологій маніпулювання квантовими системами, які зробили можливими вимір окремих квантових систем і керування ними, француз Серж Арош (Serge Haroche) і американець Девід Джей Вайнленд стали лауреатами Нобелівської премії 2012 року.

На наш погляд, у випадку появи квантового комп'ютера, що може реалізувати уже розроблені квантові алгоритми, зокрема алгоритми криптоаналізу Шора [4] та Гровера [5], можуть виникнути великі загрози у інформаційній сфері відносно забезпечення криптографічної стійкості для асиметричних криптоперетворень. При цьому важливим є не тільки сам факт побудови такого комп'ютера, а й технічні характеристики, якими буде володіти квантовий комп'ютер. Вказане необхідно враховувати, так як існуючі квантові алгоритми для своєї «роботи» потребують значних технічних ресурсів, особливо просторових у вигляді кількості кубітів [2, 4, 5].

Метою цієї статті є аналіз сучасних досягнень відносно побудови квантових комп'ютерів, оцінки можливостей реалізації на них квантових алгоритмів криптоаналізу з певними параметрами, а також оцінки і порівняння з певним прогнозуванням криптографічної стійкості асиметричних криптосистем (перетворень). Важливість цих проблемних задач пояснюється тим, що при появі квантових комп'ютерів їх застосування скоріше всього буде направлене на сучасні криптосистеми.

Сучасні криптографічні системи можна поділити на симетричні та асиметричні. У свою чергу асиметричні криптосистеми у відповідності до застосування можна поділити на системи направленого шифрування (НШ) та системи електронного цифрового підпису (ЕЦП). Класифікація існуючих криптографічних перетворень, що застосовуються для ЕЦП, наведено в табл. 1.

Таблиця 1

Асиметричні криптографічні перетворення для ЕЦП

| Параметри перетворення / Вид перетворення | Особистий ключ | Відкритий ключ (сертифікат) | Загальні параметри | Складність крипто аналізу |
|---|---|---|---|---|
| Перетворення в кільці (RSA) | $D_i$ | $E_i$ | N = PQ | Субекспоненційна |
| Перетворення в полі Галуа F(P) (DSA) | $X_i$ | $Y_i=g^{Xi}(\text{mod } P)$ | P, q, g | Субекспоненційна |
| Перетворення в групі точок еліптичних кривих E(F(q)) | $d_i$ | $Q_i=d_iG(\text{mod}q)$ | a, b, G, n, f(x)(P), h | Експоненційна |
| Перетворення в гіпереліптичних кривих | $C_i$ | $D_2= c_iD1$ | f(x), g(x), q, D1, g, J | Експоненційна |
| Перетворення зі спарюванням точок еліптичних кривих | $D_i =s_{iD}$ | $Q_{iD}$ = H1(ID) | G1, G2, e, H1, P, H2, H3, $F^{2m}$, Pp | Міжекспоненційна – субекспоненційна |
| Перетворення в фактор-кільці | f = 1+pF(modq) | (f,h) | N, q, p, f, g,df, dg, c | Експоненційна |

На сьогодні вже існують квантові алгоритми, які дають змогу проводити атаки на такі асиметричні криптосистеми:

- системи, що базуються на складності факторизації великого цілого числа (RSA) [10];
- системи, що базуються на складності вирішення дискретного логарифму в скінченному полі Галуа (DSA) [10];
- системи, що базуються на складності вирішення дискретного логарифму в групі точок еліптичної кривої (ECC) [10];
- системи на базі решіток (NTRU) [11].

Усі вказані криптосистеми відносяться до класу ймовірно-стійких. А ця ймовірна стійкість як раз і визначається можливостями появи квантових комп'ютерів, і, як наслідок, вирішення задачі повного розкриття [3].

Існують також квантові алгоритми, що можуть використовуватися для проведення криптоаналізу симетричних криптосистем, в першу чергу блокових та потокових симетричних шифрів [5].

## 3. Стан досягнень у побудові квантових комп'ютерів

Побудовою квантового комп'ютера займається багато наукових колективів та дослідних груп по усьому світу, але значних результатів у цьому напрямку, на даний момент, як свідчать дані [6, 8, 9] досягли тільки декілька колективів з США.

Так, вчені з IBM Research [8] заявили про досягнення значного прогресу у квантових обчисленнях. Вони дозволяють інженерам розпочати роботи зі створення повноцінного квантового комп'ютера. Своїми досягненнями IBM поділилися на щорічній American Physical Society. У цій роботі вченим вдалося зменшити кількість помилок при передачі даних при елементарних обчисленнях, зберігаючи при цьому цілісність квантово-механічних властивостей кубітів. Але за прогнозами до створення квантового комп'ютера поки далеко, і цей процес може зайняти від 10 до 15 років [8]. Однак для IBM результати, яких компанія досягла вже зараз, відкривають дорогу для реальних експериментів [8].

Відомо також, що дослідженнями в цій області займається не тільки IBM, але ще і Каліфорнійський і Єльський університети. Однак в IBM стверджують, що ресурси для виготовлення квантових обчислювальних чипів насправді є тільки у них [6]. При цьому, хоча поточна точність фізичних процесів становить 95 %, компанія прагне вийти на рівень точності 99 %. Це дозволить зменшити кількість помилок до прийнятного для реалізації обчислень рівня і дасть можливість масштабувати систему в цілому, забезпечуючи у цілому реалізацію більш складних проектів.

Крім того, у квітні 2012 року групі дослідників з Південно-Каліфорнійського університету [6], Технологічного університету Дельфта, університету штату Айова і Каліфорнійського університету Санта-Барбара, вдалося побудувати двохкубітний квантовий комп'ютер на кристалі алмазу з домішками. Комп'ютер функціонує при кімнатній температурі і теоретично є масштабованим. В якості двох логічних кубітів використовувалися напрямки спіна електрона і ядра азоту відповідно. Для забезпечення захисту від впливу декогерентності була розроблена ціла система, яка формувала імпульс мікрохвильового випромінювання певної тривалості і форми. За допомогою цього комп'ютера реалізований алгоритм Гровера для чотирьох варіантів перебору, що дозволило отримати правильну відповідь з першої спроби в 95 % випадків [6].

Також значних здобутків досягла фірма D-Wave, яка стала першою компанією, що продала комерційну версію квантового комп'ютера. Так з 20 травня 2011 D-Wave Systems продає за $ 11 млн доларів квантовий комп'ютер D-Wave One з 128-кубітним чіпсетом, який виконує тільки одну задачу - дискретну оптимізацію. 25 травня 2011 Lockheed Martin підписала багаторічний контракт з D-Wave Systems, що стосується виконання складних обчислювальних завдань на квантових процесорах. Контракт також включає в себе технічне обслуговування, супутні послуги і купівлю квантового комп'ютера D-Wave One [9].

У той же час необхідно відмітити, що квантові комп'ютери D-Wave Systems піддаються критиці з боку деяких дослідників. Так, професор (Associate Professor) Массачусетського Технологічного Інституту Скотт Ааронсон вважає, що D-Wave поки не змогла довести ні того, що її комп'ютер вирішує будь-які завдання швидше, ніж звичайний комп'ютер, ні того, що 128 кубітів, які використовуються, вдається ввести в стани квантової заплутаності. Якщо ж кубіти не перебувають повністю у заплутаному стані, то такий комп'ютер не можна вважати квантовим. Також необхідно відмітити, що у грудні 2012 року прорекламовано новий процесор Vesuvius, який має 512 кубітів.

У травні 2013 року професор Amherst College з канадської провінції Нова Шотландія Катерина Мак Гі оголосила про свої результати порівняння комп'ютера D Wave One (процесор Vesuvius) з чотирипроцесорним комп'ютером на основі 2,4 ГГц чіпа Intel з 16 Гб оперативної пам'яті. У першому тесті одне із завдань класу QUBO, що добре відповідає структурі процесора, комп'ютер D-Wave One виконав за 0,5 секунди, у той час як комп'ютеру з процесором Intel знадобилося 30 хвилин, тобто виграш по швидкості 3600 разів. При другому тестуванні попередньо для «перекладу» завдання на мову комп'ютера D-Wave була потрібна спеціальна програма і швидкість обчислень двох комп'ютерів була приблизно рівною. При третьому тестуванні, в якому також була потрібна програма «перекладу», комп'ютер D-Wave One за 30 хвилин знайшов рішення 28 з 33 заданих завдань, у той час як комп'ютер на базі процесора Intel знайшов рішення тільки для 9 завдань [9].

Необхідно відмітити, що для доказу того факту, що область квантових обчислень рухається вперед, вчений компанії D-Wave Зенгбінг Біен (Zhengbing Bian) використовував один з комп'ютерів компанії для вирішення дуже ресурсномісткої обчислювальної задачі побудови двобарвного графа чисел Рамсея. Як було відомо [9], з точки ресурсів та обчислювальної потужності вирішення цієї задачі для звичайного комп'ютера є неймовірно важким. Тому на вирішення цього завдання звичайному комп'ютеру середньої потужності знадобилося б 10250 років часу, а квантовому комп'ютеру D-Wave на це було потрібно всього 270 мс.

Також у травні 2013 корпорація Google оголосила про відкриття лабораторії, що пов'язана з квантовими дослідженнями у галузі штучного інтелекту. Для виконання обчислень для лабораторії був придбаний квантовий комп'ютер моделі D-Wave Two. В ньому процесор обчислювальної машини працює з 512 кубітами - квантовими бітами, які можуть знаходитися в двох станах одночасно. Безпосередньо перед укладанням угоди про постачання D-Wave було проведено випробування нової моделі комп'ютера. Незалежна експертиза підтвердила, що квантова обчислювальна машина справляється із завданнями, для яких вона була побудована, причому вона в 3600 разів обчислення веде швидше, ніж звичайний комп'ютер [12].

Раніше ряд вчених висловлював сумніви в тому, що дітище D-Wave дійсно працює за рахунок квантових ефектів і дебати про його «квантовість» тривали як мінімум кілька років. В той же час D-Wave тривалий час не висвітлювала жодної інформації щодо технічної сторони квантового комп'ютера. Але у 2013 році було певна інформація появилась у публічному доступі, в тому числі було написано декілька статей про функціонування їхнього комп'ютера.

Але, 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 ній не можуть бути реалізованими [9]. Це пов'язано з тим, що для обчислень використовується зовсім інший принцип - так звані адіабатичні квантові обчислення. Вказане значно обмежує її можливості, але дозволяє не турбуватися про декогеренції та інші проблеми, що характерні для звичайних квантових обчислювачі. Як показує аналіз, адіабатичні квантові комп'ютери являють собою спеціалізовані пристрої, що призначені для вирішення єдиного завдання: пошуку оптимального рішення функції, яка визначена енергетичним станом усіх кубітів разом. Тому виконувати операції над окремими кубітами вони не здатні.

## 4. Квантовий алгоритм Гровера та його використання для квантового криптоаналізу симетричних криптосистем

Проблема криптоаналізу симетричних криптосистем, на вирішення якої спрямовано метод Гровера, може бути сформульована наступним чином. Нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент, що володіє деякою властивістю, яка перевіряється з поліноміальною складністю. Потрібно знайти цей елемент з мінімально можливою складністю.

Для моделі пошуку k елементів, у якій виконуються вимоги відносно узагальненого парадоксу про день народження ймовірностей успіху буде k/N [13]. Отже, щоб знайти необхідний елемент з будь-якою константною (не залежної від N) ймовірністю, необхідно зробити до бази O(N) запитів. Алгоритм Гровера дозволяє знайти необхідний елемент з ймовірністю достатньо близькою до 1 за $O(\sqrt{N})$ кроків (більш точно, за $O(\sqrt{N})$ ) ітерацій виконання процедури, але за $O(\sqrt{N}\log N)$ кроків, використовуючи logN кубітів, причому logN кроків необхідно для виконання перетворення Уолша-Адамара [5].

Для вирішення цієї задачі існує значне число класичних алгоритмів, в яких для досягнення кращого результату процедура повторюється багато разів. При повторенні такої квантової процедури ймовірність успіху може збільшуватись, але після достатньої кількості повторень результат знову стає гіршим. Це можна пояснити тим, що квантова процедура - це унітарне перетворення, яке здійснює поворот в комплексному просторі. Тому повторне застосування квантового перетворення може наближати поточний стан все ближче і ближче до потрібного нам стану тільки протягом якогось числа ітерацій, подальше застосування квантового перетворення може пройти повз потрібний стан і віддалити правильне рішення. Тому, для того, щоб отримати при повторюваних квантових перетвореннях очікуваний результат, дуже важливо визначити, коли потрібно зупинитися [13].

Таким чином, з використанням алгоритму Гровера, можна знайти секретний ключ симетричного шифрування за час, де K - розмір ключа. Більш детальна оцінка стійкості симетричних систем проти квантового криптоаналізу наведена в табл. 2.

Аналіз даних таблиці показує, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму суттєво зменшується. Це означає, що DES буде повністю компрометований і не можна говорити про деяку його стійкість, так як оцінка приймає значення $2^{28}$. Також видно, що навіть при AES-128 можна було б знайти секретний ключ за час, приблизно $2^{64}$. А $2^{64}$ нині уже вважається небезпечним значенням.

Таблиця 2

Стійкість симетричних криптосистем проти квантового криптоаналізу

| № п/п | Шифр | Розмір блока/ключа, біт | Кількість необхідної пам'яті для атаки на блок повідомлення/ключ, кубіт | Стійкість при атаці на | |
|---|---|---|---|---|---|
| | | | | блок повідомлення | ключ |
| 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 | $2^{32}$ ($10^{9,6}$) | $2^{224}$ ($10^{67,2}$) |

Що стосується AES-256 біт, то часова складність роботи алгоритму Гровера становить $2^{128}$, що є допустимим при нинішніх поглядах. Що стосується ДСТУ ГОСТ 28157-2009 (ГОСТ 28147-89) , то оскільки в ньому довжина блоку 64 біта і розмір ключа 256 біт, то при атаці на блок повідомлення стійкість буде $2^{32}$, а при атаці на ключ - $2^{128}$.

Таким чином, по суті, алгоритм Гровера дозволяє реалізувати алгоритм узагальненого парадоксу про день народження.

## 5. Квантовий алгоритм факторизації Шора

На нинішній час широке розповсюдження та застосування знайшов алгоритм асиметричного перетворення в кільці, який отримав назву RSA перетворення. За складністю основним етапом його криптоаналізу, тобто знаходження особистого ключа, є факторизації модуля перетворення N [2, 14]. Усі відомі нині 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. Але застосування алгоритму загального або спеціального решета числового поля для реальних значень загальних параметрів, наприклад $N \geq 2^{2048}$, не можуть бути реалізовані. Часова складність таких алгоритмів оцінюється як субекспоненційна, наприклад у вигляді [2]:

$$O(\exp((c+o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3})). \quad (1)$$

В той же час квантовий алгоритм Шора, що ним запропонований і розглядається нижче, має поліноміальну складність. Він здатен розкласти складене число на прості множники приблизно за такий час $O(n^3)$ та з використанням $O(n)$ кубітів [4]. Розглянемо його детальніше.

Поліноміальний за часом алгоритм Шора, що запропонований ним в 1994 році, дозволяє факторизувати N - значне число на квантовому комп'ютері з певною ймовірністю та з обмеженою помилкою. Пропозиція та оцінки складності алгоритму Шора вразили, пробудивши широкий інтерес до квантових обчислень. Більшість алгоритмів криптографів. 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 N, який використовується для його факторизації. З точки зору складності, найбільшу трудність становить перетворення Фур'є, що базується на алгоритмі швидкого перетворення Фур'є.

Шор також показав, що його дозволяє розкласти число N з часовою складністю $O(\log^2 N \log^3(\log N))$ з використанням $O(\log N)$ логічних кубітів [13].

Таким чином, значимість алгоритму полягає в тому, що при використанні квантового комп'ютера з декількома сотнями логічних кубітів він дозволяє, наприклад, зламати RSA криптоперетворення, розклавши модуль перетворення N, тобто знайти множники модуля N. Уже при $N \geq 21^{024}$ це зробити практично неможливо, якщо використовувати відомі класичні алгоритми.

Попередні оцінки показують, що алгоритм Шора дозволить вирішити проблему факторизації числа N за допомогою вирішення еквівалентної проблеми – для певного числа a, що є взаємно простим з N, знайти порядок r елемента a mod N. При цьому ціле число a рекомендується вибирати випадково і рівно ймовірно. Далі, використовуючи Алгоритм Евкліда, можна визначити, чи a взаємно просте з N. Якщо a не є взаємно простим з N, то буде знайдено дільник числа N. В іншому випадку, порядок r елемента a mod N буде дільником числа N.

Порівняльний аналіз класичного алгоритму і квантового алгоритмів факторизації наведено у табл. 3.

Таблиця 3

Порівняльний аналіз класичного алгоритму і квантового факторизації (RSA)

| Алгоритм факторизації RSA | | | |
|---|---|---|---|
| Розмір модуля, бітів | Кількість необхідних кубітів $2n$ | Складність квантового алгоритму $4n^3$ | Складність класичного алгоритму |
| 512 | 1024 | $0.54 \cdot 10^9$ | $1.6 \cdot 10^{19}$ |
| 768 | 1536 | $1.8 \cdot 10^9$ | $9.9 \cdot 10^{22}$ |
| 1024 | 2048 | $4.3 \cdot 10^9$ | $1.2 \cdot 10^{26}$ |
| 2048 | 4096 | $34 \cdot 10^9$ | $1.35 \cdot 10^{35}$ |
| 3072 | 6144 | $12 \cdot 10^{10}$ | $5 \cdot 10^{41}$ |
| 15360 | 30720 | $1.5 \cdot 10^{13}$ | $9.2 \cdot 10^{80}$ |

Аналіз даних табл. 3 показує, що для зламу RSA криптосистеми з розміром модуля у 15360 бітів (розмір головного сертифікату відкритого ключа США), необхідно лише $1.5 \cdot 10^{13}$ операцій на квантовому комп'ютері, тоді як класична обчислювальна система повинна виконати порядку $10^{80}$ операцій. Тобто RSA система буде зламана за поліноміальний час. Крім того, як слідує із табл. 3, навіть суттєве збільшення модуля, наприклад $2^{3072}$ та більше, не врятовує RSA криптосистему від її злому.

## 6. Квантовій алгоритм Шора дискретного логарифму в скінченному полі та в групі точок еліптичної кривої

Проведений аналіз показує [4], що алгоритм Шора дискретного логарифмування в групі точок еліптичної кривої та в скінченному полі має однакові кроки, єдине в чому різниця – це представлення точок еліптичної кривої та елементів поля.

Розглянемо їх криптографічну стійкість та зробимо відповідні оцінки для них. Нині вважається, що вирішення задач дискретного логарифмування в групі точок еліптичних кривих найбільш ефективно може бути реалізованим з використанням ρ- та λ - методів Полларда [2]. Для них складність можна оцінити як:

$$O(\sqrt{q}), \quad (2)$$

де q - кількість точок еліптичної кривої.

В той же час квантовий алгоритм Шора у загальному випадку має поліноміальну складність вирішення такого класу задач, як, наприклад, факторизації. Так, він здатен розв'язати логарифмічне рівняння приблизно за такий час $O(n^3)$ та з використанням $O(n)$ кубітів, де n - розмір базової точки. Детальний порівняльний аналіз класичних алгоритмів та квантового алгоритму Шора наведений у табл. 4 [4, 15].

Таблиця 4

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

| Алгоритм розв'язку дискретного логарифмічного рівняння | | | |
|---|---|---|---|
| Розмір порядку базової точки, бітів | Кількість необхідних кубітів $f(n) = 7n + 4\log_2 n + 10$ | Складність квантового алгоритму $360n^3$ | 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. 4 видно, що навіть збільшення розміру порядку базової точки при криптоаналізі з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості криптографічної системи на еліптичних кривих. Також видно, що при збільшені 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 все одно тривалий час буде недоступною.

На сьогодні «рекордом класичного криптоаналізу» в групі точок еліптичних кривих є рішення дискретного логарифмічного рівняння в полі $GF(2^{109})$ [2], при розмірі базової точки 108 бітів. Така задача була розв'язана у 2000 році французькими криптологами, для її вирішення знадобилося 9500 комп'ютерів та трохи більше 4 місяців.

Також нині існує багато алгоритмів та методів, за допомогою яких можна знайти розв'язок дискретного логарифму в скінченному полі. Найкращим класичним алгоритмом дискретного логарифмування в скінченному полі є метод решета числового поля. Для нього складність можна оцінити як [2]:

$$O(\exp(3^{3/2}(\ln(P)\ln(\ln(P)))^{1/3}). \quad (3)$$

Але, як слідує із [2], класичні методи криптоаналізу систем направленого мають субекспоненційну або експоненційну складність. В той же час алгоритм Шора, маючи поліноміальну складність, дозволяє вирішити проблему дискретного логарифму в полі з суттєво меншою складністю [15]. Порівняльний аналіз складності алгоритму решета числового поля та алгоритму Шора дискретного логарифмування в скінченному полі наведено в табл. 5.

Таблиця 5

Порівняльний аналіз класичного і квантового алгоритму дискретного логарифмування в скінченному полі

| Алгоритм розв'язку дискретного логарифмічного рівняння | | | |
|---|---|---|---|
| Розмір модуля перетворення, бітів | Кількість необхідних кубітів $\approx 3n$ | Час квантового алгоритму $\approx n^3$ | Час класичного алгоритму |
| 512 | 1536 | $1.3\cdot10^8$ | $4.9\cdot10^{15}$ |
| 1024 | 3072 | $0.1\cdot10^{10}$ | $3.3\cdot10^{20}$ |
| 2048 | 6144 | $0.9\cdot10^{10}$ | $5.3\cdot10^{26}$ |
| 3072 | 9216 | $2.9\cdot10^{10}$ | $1.4\cdot10^{31}$ |
| 8162 | 24486 | $0.5\cdot10^{12}$ | $8.2\cdot10^{44}$ |
| 15360 | 46080 | $3.6\cdot10^{12}$ | $5.9\cdot10^{56}$ |

Із табл. 5 видно, що збільшення розміру модуля перетворення і, відповідно, особистого ключа, не забезпечує необхідного збільшення складності дискретного логарифмування в скінченному полі, наприклад, при зломі електронного цифрового підпису чи направленого шифрування. Так, для модуля $P \geq 2^{3072}$ складність дискретного от логарифмування в скінченному полі складає $1.4\cdot10^{31}$, а з застосуванням алгоритму Шора всього $2.9\cdot10^{10}$ операцій. Але для квантового алгоритму залишається велика кількість кубітів, яка необхідна для проведення квантової атаки. Скоріше всього вона тривалий час буде недоступною.

## 7. Квантовий алгоритм криптоаналізу перетворень в фактор кільці

Криптографічне перетворення в фактор – кільці використовується при реалізації асиметричної криптографічної системи направленого шифрування NTRU [16]. У 1996 році вона була визнана у IEEE P1363 та EESS (Consortium for Efficient Embedded Security), як одна із стандартних систем з відкритим ключем. Особливістю алгоритму NTRU є суттєве зменшення складності прямого та зворотного перетворень, тобто можливість підвищення швидкодії [11, 16].

Але для застосування NTRU необхідно доводити її криптографічну стійкість. Також було з'ясовано, що при реалізації атак на класичних комп'ютерах складність пошуку особистого ключа направленого шифрування носить експоненційний характер [17]. Тому великий інтерес був проявлений до вивчення можливостей використання для здійснення атак квантового комп'ютера.

У 2003 році Людвіг [18] застосував квантовий алгоритм пошуку Гровера на основі решіток. Ним було виявлено, що час роботи квантового алгоритму пошуку (QRS) у порівнянні з класичними алгоритмами різко, але все ще мав експоненційну часову складність. У 2005 році Грехем вказав, що обчислювальна складність QRS

більша, ніж у атаки зустріч посередині. У 2009 році NTRU також вважався безпечним відносно квантових атак. Але у 2010 році Ванг [19] запропонував квантовий алгоритм пошуку цільового рішення з фіксованою вагою, і застосував його для пошуку особистого ключа NTRU. В той же час метод Ванга потребує малого обсягу зберігання даних, але складність обчислень у нього ще більше, ніж у атаки зустріч посередині.

Аналіз показує [20], що нині атака зустріч посередині є найбільш ефективним методом пошуку NTRU особистого ключа, але його часова складність до сих пір дуже велика. Як слідує із [19], метод Ванга може розглядатися, як алгоритм квантового пошуку типу «груба сила», але який зменшує часову складність з $O(C_N^{d_f})$ до $O(\sqrt{C_{N+1}^{d_f}})$.

Вказане може бути ефективно застосовано для комбінації квантових обчислень з атакою зустріч посередині. Такий метод і на його основі алгоритм був запропонований у роботі Ксіонга [20] у 2012 році, проте у 2013 році Ванг написав статтю [21], у якій було вказано на суттєві недоліки пропозицій Ксіонга. У цій же статті Ванг запропонував удосконалення атаки на систему NTRU. Основний недолік роботи Ксіонга – це те, що в його методі не вказана складність виконання необхідних передобчислень, хоча їх складність є суттєвою і складність таких передобчислень у Ксіонга більше, ніж у Ванга.

Аналітичні співвідношення оцінки складності атак на систему NTRU наведено у табл. 6 [21].

В табл. 6 для останніх 2 стовпців під $\bar{O}$ мається на увазі складність квантової атаки зустріч посередині, а під O складність обрахунку таблиці передобчисленням для виконання атаки. З табл. 6 видно, що складність побудови таблиці передобчислень дуже велика і неможна її не враховувати при аналізі складності атаки.

Порівняльний аналіз часової складності для різних розмірів системних параметрів NTRU та різних атак наведено у табл. 7.

Дані табл. 7 дозволяють зробити такі висновки відносно складності алгоритмів криптоаналізу криптографічних перетворень в фактор – кільці (NTRU). Удосконалена квантова атака методом Ванга має суттєво меншу складність ніж складність квантової атаки методом Ксіонга, а також меншу складність ніж складність класичної атаки методом зустріч посередині.

Складність квантової атаки методом Ксіонга більше складності атаки методом Ванга і суттєво більше за класичну атаку зустріч посередині [21].

Для реалізації квантової атаки метод Ванга (зустріч посередині) необхідно будувати таблиці переобчислень, складність яких значна і потрібно враховувати при аналізі складності атаки в цілому.

## 8. Висновки та рекомендації

1. Незважаючи на особливу складність практичного розроблення «істинно квантового» комп'ютера, в цьому напряму ведуться інтенсивні дослідження і отримано ряд важливих результатів, що вимагає врахування при проектуванні та застосуванні можливостей здійснення ефективних атак на асиметричні системи криптографічних перетворень в кільцях та скінченних полях. В цілому враховуючи темпи розвитку і досліджень в області квантових обчислень, скоріше за все сучасні криптосистеми стануть вразливими для квантових атак.

2. Забезпечення необхідного рівня стійкості симетричних криптографічних систем при появі квантового комп'ютера можна тільки за допомогою збільшення розмірів довжини блока та довжини ключа.

Але і за умови збільшення розмірів системних параметрів симетричні системи можуть бути при певних параметрах уразливими для квантового криптоаналізу.

Таблиця 6

Часова та просторова складність основних атак на NTRU

| | Груба сила | Класична атака зустріч посередині | Атака методом Ванга | Квантова атака зустріч посередині (метод Ксіонга) | Удосконалена квантова атака зустріч посередині (метод Ванга) |
|---|---|---|---|---|---|
| Часова складність | $O(C_N^d)$ | $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$ | $O(\sqrt{C_{N+1}^d})$ | $O(C_{N/2}^{d/2}\log C_{N/2}^{d/2}) + \bar{O}\sqrt{C_{N/2+1}^{d/2}}$ | $O(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\log C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}) + \bar{O}\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}}$ |
| Просторова складність | O(1) | $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$ | O(1) | $O(C_{N/2}^{d/2})$ | $O(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor})$ |

Таблиця 7

Часова складність різних алгоритмів криптоаналізу NTRU

| Параметри NTRU | Груба сила | Класична атака зустріч посередині | Атака методом Ванга | Квантова атака зустріч посередині (метод Ксіонга) | Удосконалена квантова атака зустріч посередині (метод Ванга) |
|---|---|---|---|---|---|
| NTRU251 | $10^{52}$ | $10^{24}$ | $10^{26}$ | $3.3\cdot10^{27}+7\cdot10^{12}$ | $3.5\cdot10^{18}+1.6\cdot10^{17}$ |
| NTRU347 | $10^{72}$ | $10^{34}$ | $10^{36}$ | $4.6\cdot10^{37}+6.9\cdot10^{17}$ | $9\cdot10^{25}+7.6\cdot10^{23}$ |
| NTRU491 | $10^{100}$ | $10^{48}$ | $10^{50}$ | $3.2\cdot10^{52}+1.5\cdot10^{25}$ | $3\cdot10^{35}+1.8\cdot10^{33}$ |
| NTRU587 | $10^{120}$ | $10^{58}$ | $10^{60}$ | $4.5\cdot10^{60}+7.6\cdot10^{29}$ | $3.8\cdot10^{41}+9\cdot10^{39}$ |
| NTRU787 | $10^{159}$ | $10^{77}$ | $10^{79}$ | $1.5\cdot10^{81}+2.7\cdot10^{39}$ | $4.6\cdot10^{54}+3.7\cdot10^{52}$ |

3. Складність вирішення задач факторизації в кільцях та дискретного логарифмування в скінченному полі при застосуванні класичних комп'ютерів носить в кращому випадку субекспоненційний характер. Поява нових математичних методів факторизації та дискретного логарифмування та їх практична реалізація можуть привести до того , що перетворення в кільці та в скінченному полі будуть не стійкими до атак типу «повне розкриття».

4. Складність задач дискретного логарифмування в групі точок еліптичних кривих носить експоненційний характер. Мінімальна складність дискретного логарифмування в групі точок еліптичних кривих може бути реалізованою з використанням ρ- та λ - методів Полларда.

5. Квантовий алгоритм Шора у загальному випадку має поліноміальну складність вирішення задач криптоаналізу, наприклад факторизації чи дискретного логарифмування. При його застосуванні складність дискретного логарифмування складає час $O(n^3)$ та використання O(n) кубітів, де n – порядок базової точки.

6. Збільшення загальних параметрів асиметричних криптосистем не дає суттєвого збільшення стійкості таких систем. Так для зламу криптосистеми на базі еліптичних кривих з розміром базової точки у 512 бітів необхідно усього лише $50 \cdot 10^9$ оп. на квантовому комп'ютері, а при збільшенні розміру базової точки до 1024 бітів складність криптоаналізу збільшиться до $3.8 \cdot 10^{11}$ оп., тобто зростає несуттєво. Єдине на чому може базуватися стійкість асиметричних криптосистем при квантовому крипто аналізі – це те, що в найближчі роки не з'являться квантові комп'ютері з необхідним для цього числом кубітів.

7. Необхідно відмітити, що для забезпечення криптографічної стійкості перетворень в групі точок еліптичних кривих в перспективі необхідно збільшувати розміри загальних параметрів, з порядком базових точок навіть 1024 бітів. Вказане вимагає безперервного відслідковування та прогнозування стійкості усіх асиметричних криптоперетворень, а також та своєчасного збільшення.

8. Можливості реалізації квантові обчислення також суттєво впливають на стійкість крипто перетворень в фактор – кільцях (кільцях зрізаних поліномів). Так комбінуючи атаку зустріч посередині і квантовий алгоритм пошуку Гровера, можна здійснити квантову атаку зустріч посередині, що потребує значно менших затрат, ніж аналогічна класична атака на криптосистему типу NTRU.

9. Криптосистеми на базі NTRU можуть стати уразливими до квантового криптоаналізу, хочу ще не так давно зазначалося, що такі схеми будуть стійкі проти нього. Так квантова атака «зустріч посередині» у разі появи квантових комп'ютерів може компрометувати системи на основі фактор – кілець (NTRU).

10. Особливу увагу необхідно приділяти оцінці стійкості криптографічних систем та протоколів, що ґрунтуються на перетвореннях в групі точок еліптичних кривих. Це можна пояснити тим, що на них реалізовані та широко застосовуються системи цифрового підпису, протоколів автентифікації, встановлення ключів, направленого шифрування тощо.

Література


1. Feyman, R. P. Quantum mechanical computers [Text] / R. P. Feyman // Opt. News – 1985. - February.11. - pp.. 11-39.
2. Горбенко, І. Д. Прикладна криптологія. [Текст]: монографія / І. Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. - 868 с.
3. Deutsch, D. Rapid Solution of problems by quantum computation [Text] / Deutsch, D. , Jozsa R. // Proc. R. Soc. Lond. A. – 1992. – Vol. 439 (1907). – pp.553-558.
4. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text] / P. W. Shor //SIAM J. Comput. - 1997. - 26 (5). - pp. 1484–1509.
5. 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. - pp. 212-219.
6. Quantum computer built inside diamond [Electronic resource] / Futurity Research news from top universities- Режим доступа: \www/ URL: – http://www.futurity.org/quantum-computer-built-inside-diamond/ - 09.04.2012.
7. Dalfovo, F. V. Theory of Bose-Einstein condensationin trapped gases [Text] / Dalfovo F. , Giorgini S. , Pitaevskii L. P. , Stringari S. // Rev. Mod, Physics. – 1998 -71, No3. - pp. 463-510.
8. IBM Research Advances Device Performance for Quantum Computing [Electronic resource] / NY. IBM news - Режим доступа: \www/ URL: – http://www-03.ibm.com/press/us/en/pressrelease/36901.wss - 28.02.2012 р.
9. Lockheed Martin piece about D-Wave technology [Electronic resource] / Burnaby, British Columbia, Canada Блог компанії D-Wave Режим доступа: \www/ URL: – http://dwave.wordpress.com/2013/03/08/lockheed-martin-piece-about-d-wave-technology/. - 08.03.2013 р.
10. FIPS-186-3. Digital signature standard: 2009 [Text]. 2009 – 07 – 19 - Gaithersburg, MD 20899-8900 - 2009 – 120 p.
11. 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.
12. 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.
13. Гайнутдинова, А. Ф. Квантовые вычисления [Текст]: метод.пособие. А. Ф. Гайнутдинова. – Казань: Казанский государственный университет, 2009, - 272 с.

14. Lenstra H. W. Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory [Text] / H. W. Lenstra, Jr. and R. Tijdeman, eds.// Math. Centre Tract 154 - 1946 - pp. 89-139.
15. Proos, J. Shor's discrete logarithm quantum algorithm for elliptic curves [Text] / Proos J., Zalka C. // QIC. – 2003. – Vol.4. – pp. 317-344.
16. Hoffstein, J. NTRU: A ring-based public key cryptosysytem [Text] / J. J. Pipher and J. Silverman // ANTS III. – 1998 – Vol.1423 – pp. 267-288.
17. Silverman, J. A Meet-The Middle Attack on an NTRU Private Key [Text] / J. Silverman, J. Odlyzko // NTRU Cryptosysytems. - Technical Report, NTRU Report - 2003 - 004, Version 2. – 7 p.
18. Ludwig, C. A faster lattice reduction method using quantum search [Text] / C. A. Ludwig // Algo Comput, - 2003 – Vol.2906. – pp. 199-208.
19. Wang, X. A quantum algorithm for searching a target solution of fixed weight [Text] / Wang, X. W. , S. Bao and X. Q. Fu// Chinese Sci Bull. - 2010.- Vol.55(29). – pp.484-488.
20. Xiong, Z. An Improved MITM Attack Against NTRU [Text] / Z. Xiong Wang J. , Wang Y. , Zhang T. , Chen L. // International Journal of Security and Its Applications. – 2012. - Vol. 6, No. 2. – pp. 269-274.
21. Wang, H. An efficient quantum meet-in-the-middle attack against NTRU-2005 [Text] / Wang Hong, MA Zhi, MA ChuanGui // Chinese Science Bulletin. – 2013. - Vol. 58, No.28-29. – pp.3514-3518.

***Обґрунтовується вибір циклових функцій у схемі доказовою стійкого ключового універсального гешування, пропонується модель і метод формування кодів контролю цілісності та автентичності даних на основі модулярних перетворень, алгоритм зниження обчислювальної складності реалізації схем гешування з використанням циклових функцій. Розроблений вдосконалений алгоритм UMAC забезпечує необхідні показники колізійних властивостей універсального гешування, доказовий рівень стійкості і високі показники швидкодії***

***Ключові слова: коди контролю цілісності та автентичності даних, модулярні перетворення, універсальні класи геш-функцій***

***Обосновывается выбор цикловых функций в схеме доказуемо стойкого ключевого универсального хеширования, предлагается модель и метод формирования кодов контроля целостности и аутентичности данных на основе модулярных преобразований, алгоритм снижения вычислительной сложности реализации схем хеширования с использованием цикловых функций. Разработанный усовершенствованный алгоритм UMAC обеспечивает требуемые показатели коллизионных свойств универсального хеширования, доказуемый уровень стойкости и высокие показатели быстродействия***

***Ключевые слова: коды контроля целостности и аутентичности данных, модулярные преобразования, универсальные классы хеш-функций***

УДК 681.3.06 (0.43)

# УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ UMAC НА ОСНОВЕ МОДУЛЯРНЫХ ПРЕОБРАЗОВАНИЙ

**С. П. Евсеев**
Кандидат технических наук, доцент*
E-mail: Evseev_Serg@inbox.ru.
**О. Г. Король**
Преподаватель*
E-mail: korol_o@mail.ru
**В. В. Огурцов**
Кандидат экономических наук, доцент*
*Кафедра информационных систем
Харьковский национальный экономический университет им. С. Кузнеца
пр. Ленина 9-а, Харьков, Украина, 61166
E-mail: Vitalii.Ohurtsov@hneu.net или vetalreal@ukr.net

## 1. Введение

Проведенные исследования показали, что использование модулярных преобразований позволяет реализовать доказуемо стойкое хеширование информации, удовлетворяющее коллизионным свойствам универсальных хеш-функций. Доказуемо безопасный уровень стойкости обосновывается сведением