УДК 004.056

В.С. Бурковський

*Харківський національний університет радіоелектроніки, Харків*

# ОГЛЯД МОЖЛИВОСТЕЙ КВАНТОВОГО КРИПТОАНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЛАТФОРМ, ЩО Є СТІЙКИМИ ДО НЬОГО ТА МОЖУТЬ БУТИ ОСНОВОЮ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

*Представлена порівняльна оцінка складності алгоритмів криптоаналізу на квантовому та класичному комп'ютері. Розглядаються криптографічні платформи, що є стійкими до квантового криптоаналізу та можуть бути основою для систем електронного цифрового підпису.*

***Ключові слова:*** *алгоритм квантовий, алгоритм Шора, алгоритм Гровера, електронний цифровий підпис, постквантова криптографічна платформа.*

## Вступ

Сучасні криптографічні системи поділяються на симетричні та асиметричні. У свою чергу, асиметричні криптосистеми поділяються на системи направленого шифрування та системи електронного цифрового підпису (ЕЦП). Ймовірна стійкість сучасних систем ЕЦП в значній мірі визначається ймовірністю появи квантових комп'ютерів [1].

На теперішній час вже існують квантові алгоритми Шора та Гровера за допомогою яких можна здійснити криптоаналіз всіх ЕЦП, що наведені в [2]. Криптостійкість ЕЦП базуються на складності:

– факторизації великого цілого числа (RSA);

– вирішення дискретного логарифму в кінцевому полі Галуа (DSA);

– вирішення дискретного логарифму в групі точок еліптичної кривої (ECC).

Існують також квантові алгоритми, що можуть використовуватися для проведення криптоаналізу симетричних криптосистем, в першу чергу, блокових та потокових симетричних шифрів [3].

Алгоритм факторизації Шора та його модифікація для дискретного логарифмування представлені в статтях [4 – 6]. Інформація по рішенню ECDLP на квантовому комп'ютері приведена в роботі [7]. Опис та інтерпретація алгоритму Гровера представлені в роботах [3; 8]. Методи факторизації та дискретного логарифмування для класичного комп'ютера наведені в роботах [9 – 11]. Детальний огляд класичних арифметичних алгоритмів наведений в [12].

Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем наведений в роботах [13; 14].

**Метою статті є:**

– проведення порівняльного аналізу потрібних ресурсів класичних та квантових алгоритмів криптоаналізу, а також їх порівняння з ресурсами сучасних та перспективних квантових комп'ютерів;

– огляд криптографічних платформ**,** що будуть стійкими після появи квантового комп'ютера с достатнім числом кубітів та можуть бути основою для побудови систем ЕЦП.

## Основна частина

**Порівняльна оцінка складності алгоритмів криптоаналізу на квантовому та класичному комп'ютері**.

У випадку появи квантового комп'ютера, на ньому будуть реалізовані уже розроблені квантові алгоритми криптоаналізу Шора [5] та Гровера [3].

Для реалізації квантового алгоритму Шора [14] необхідно здійснити дві основні квантові операції: піднесення до ступеню та квантове дискретне перетворення Фур'є. Асимптотичне кращим алгоритмом множення для масивів вентилів є алгоритм Шонхаге-Штрассена. Його квантова версія дозволяє побудувати масив квантових вентилів об'єму $O(l \log(l) \log(\log(l)))$ для піднесення до ступеню по модулю, який вирішує задачу за час $O(l^2 \log(l) \log(\log(l)))$. Тут $l$ — кількість біт в двійковому зображенні числа n, що буде факторизовано. Квантове дискретне перетворення Фур'є у відповідності до квантової версії класичної ідеї Кули-Тьюки швидкого перетворення Фур'є потребує $O(l^2)$ квантових вентилів ($O(l \log l)$, якщо обчислюється наближене QFT). Шор показав, що його алгоритм вирішує задачу факторизації з імовірністю $(1-\varepsilon)$ за N прогонів базового алгоритму:

$$N \geq l^2 (2 \log (1/\varepsilon))/ (\alpha \beta),$$

де $\alpha$ и $\beta$ – незалежні константи відносно n. В роботі [4] оцінка для N уточнена для випадку двох простих співмножників.

Якщо $n = p\,q$, а p и q прості числа, то

$$N \geq l (2 \log (1/\varepsilon))/(\alpha (1-(2+2^{\min(\tau p, \tau q)})/(3\, 2^{\tau p+\tau q})),$$

де $p-1=2^{\tau p}\sigma_p$, $q-1=2^{\tau q}\sigma_q$, а $\sigma_p$ и $\sigma_q$ такі непарні числа, що $\tau p, \tau q \geq 1$. Таким чином, квантовий час роботи базового алгоритму факторизації Шора (однієї ітерації загального алгоритму) поліноміально залежить від $l$ та складає $O(l^2 \log(l) \log(\log(l)))$. Це створює загрозу всієї асиметричної криптографії.

Однак, для симетричної криптографії та хешування цей алгоритм не підходить, а єдиним універсальним алгоритмом, що придатний для будь-якої симетричної криптографії та хешування це алгоритм Гровера. По суті, алгоритм Гровера дозволяє реалізувати алгоритм узагальненого парадоксу про день народження. Для моделі пошуку k елементів, у якій виконуються вимоги відносно узагальненого парадоксу про день народження, ймовірність успіху буде дорівнювати k/N [15]. Алгоритм Гровера дозволяє знайти необхідний елемент з ймовірністю достатньо близькою до 1 за $O(\sqrt{N})$ кроків. Більш точно з використанням ітераційної процедури, але за $O(\sqrt{N}\log(N))$ кроків, використовуючи log(N) кубітів, причому log(N) кроків необхідно для виконання перетворення Уолша-Адамара [3].

Для класичних комп'ютерів не існує алгоритмів, що працюють за поліноміальний час. Найбільш ефективні алгоритми досягають лише субекспоненціальної часової складності за рахунок використання факторної бази. В роботі таких алгоритмів розрізняються два основних етапи. На першому, підготовчому, формується факторна база та на її основі генерується система лінійних рівнянь в кільце $\mathbf{Z}_{p-1}$. Вид факторної бази (множина простих чисел багаточленів, що не приводяться, або інших об'єктів) і способи отримання матриці системи залежать від обраного алгоритму. На другому етапі (який є загальним для цих алгоритмів) отримуються рішення цієї системи. Підготовчий етап для кожного поля достатньо виконати тільки один раз, після чого можна швидко обчислювати факторизацію чисел та різні дискретні логарифми.

Субекспоненціальну складність описують L-нотацією [16]:

$$L_n[\gamma; c] = \exp(c + O(1)) \cdot \log(n)^{\gamma} \cdot \log(\log(n))^{1-\gamma},$$

$$\text{При } 0 < \gamma < 1 \text{ и } c=\text{const}, c > 0,$$

де n – число, яке необхідно факторизувати.

На теперішній час самими ефективними алгоритмами факторизації числа $n>10^{110}$ є варіації алгоритмів, заснованих на методі решета числового поля [25]:

– спеціальний метод решета числового поля SNFS (special number field sieve), що має складність $L_n[1/3; (32/9)^{1/3}]$ (цей метод може застосовуватись лише для факторизації чисел спеціального виду) [9];

– загальний метод решета числового поля GNFS (general number field sieve), що має складність $L_n[1/3; (64/9)^{1/3}]$ [11].

До того найшвидшим був алгоритм квадратичного решета QS (quadratic sieve algorithm). Він і нині найшвидший при факторизації чисел $n<10^{110}$ [13]. Його складність оцінюють як $L_n[1/2; 1]$. Зараз, у алгоритмі факторизації за допомогою еліптичних кривих така сама складність, як і в QS (у випадку, якщо n є добуток лише двох простих чисел), однак на практиці QS швидше, оскільки він використовує операції одинарної точності замість операцій довгої арифметики, які використовуються в методі еліптичних кривих.

Алгоритм Ленстри заснований на методі факторизації з використанням еліптичних кривих ECM (elliptic curve method). Часову складність алгоритму оцінюють як $L_p[1/2; 2^{1/2}]$, де

$$Lp[\gamma; c] = \exp((c+o(1))\, p^{\gamma}\, (\log(p))^{\gamma}\, (\log(\log(p))^{1-\gamma}),$$

де p – найменший дільник числа n, яке необхідно факторизувати.

Цей час буде забезпечений у випадку, якщо межа $B_1$ обрана близько до величини $\exp((1/2^{1/2} +o(1))\, (p \log(p) \log(\log(p))^{1/2})$. Оскільки значення дільника p невідомо, то вибір значення $B_1$ виконують емпірично, що дещо погіршує практичну оцінку збіжності. Додавання в алгоритм другої стадії обчислень зберігає загальну асимптотичну оцінку, хоча не забезпечує великий практичний приріст швидкості збіжності алгоритму.

Результат порівняння ECM з методами QS та GNFS залежить від розміру найменшого дільника числа n. Якщо число n обрано як визначено в RSA у вигляді добутку двох простих чисел приблизно однакової довжині, то метод ECM має таку ж оцінку, що і метод QS, однак поступається методу GNFS. Однак, якщо n має розмірність, що перевищує рекордні показники для методів QS та GNFS, (у 2009 році рекордна факторизація чисел RSA довжини 768 біт), то єдина надія знайти дільник n тільки на ECM.

На теперішній час найбільш ефективними для вирішення задачі дискретного логарифмування в полі (кільці) лишків по модулю простого числа є два наступних алгоритми:

– алгоритм COS (Coppersmith, Odlyzko, Schroeppel) [17], що має евристичну оцінку складності $L_n[1/2; 1]$ операцій (ефективне при $n<10^{90}$);

– загальний алгоритм решета числового поля (GNFS) [18] при $n>10^{100}$ більш ефективний, ніж різні модифікації методу COS, та має складність порядку $L_n[1/3; (64/9)^{1/3}]$ арифметичних операцій.

Для рішення задачі дискретного логарифмування в довільному кінцевому полі GF(q) (полі Галуа) використовують наступні три алгоритми:

– алгоритм обчислення порядку "*index-calculus algorithm*", запропонований Адлеманом [19] та має складність $L_n[1/2; c]$ при обчисленні дискретного логарифму в простому полі $\mathbf{Z}_p$;

– алгоритм Ель-Гамаля, який застосовується в кінцевому полі характеристики 2 та має складність $L_n[1/2; c]$ арифметичних операцій;

– алгоритм Копперсміта дискретного логарифмування в кінцевому полі характеристики 2, який був першим субекспоненціальним алгоритмом з константою c=1/3 в оцінці складності.

Для проблеми дискретного логарифмування в

групі точок загальної еліптичної кривої (ECDLP) на класичному комп'ютері не існує субекспоненціального алгоритму. Існують лише експоненціальні алгоритми. Найшвидшими є алгоритм Шенкса та ρ-метод Полларда (у обох часова складність $O(n^{1/2})$). Побудувати субекспоненціальні алгоритми на тих принципах, використання яких призвело до успіху у вирішення задачі дискретного логарифмування в полі (кольці), неможливо, оскільки для еліптичних кривих не знайдено факторної бази (немає аналогів простих чисел або багаточленів, що не приводяться). Тому складність рішення ECDLP на класичному комп'ютері визначається складністю $\lambda$-методу Полларду і складає $(\pi\ 2^l)^{1/2}$ операцій. Використання $\lambda$-методу обумовлено тим, що у порівнянні з $\rho$-методом він має наступні переваги. По-перше, він добро розпаралелюється [20] у великих розподілених обчислювальних системах типу Інтернет, оскільки на відміну від $\rho$-методу не потребує постійного контакту з сервером. По-друге, складність $\lambda$-методу дорівнює квадратному кореню з довжини інтервалу, який містить рішення задачі дискретного логарифмування, та якщо є апріорна інформація, що рішення задачі не розподілене рівномірно у всьому інтервалі від 1 до n-1, то його можна знайти значно швидше. Саме $\lambda$-метод був використаний в квітні 2000 року для рішення задачі ECDLP кривої $y^2 + x \cdot y = x^3 + x^2 + 1$ над полем $GF(2^{109})$, порядок якої всього 108 біт, у рамках міжнародного проекту. Задача була вирішена за 4 місяці за допомогою 9500 комп'ютерів з використанням ресурсів Інтернету. Цього об'єму обчислень вистачило б для рішення 50 задач факторизації 512-бітових чисел. Цей приклад ілюструє різницю між алгоритмами експоненціальної та субекспоненціальної складності.

**Оцінка об'єму потрібних ресурсів.**

В табл. 1 і 2 приведена оцінка потрібних ресурсів для рішення задач ECDLP и факторизації [2; 14].

Таблиця 1

Потрібні ресурси для ECDLP

| Квантовий комп'ютер | | | Класичний комп'ютер |
|---|---|---|---|
| Квантовий алгоритм ECDLP модифікація схеми Борегарду | | | Алгоритм ρ-методу Полларду |
| ключ, біт | розмір регістру, кубіт | кількість квантових операцій | кількість класичних операцій |
| $l$ | $5l+8l^{1/2}+2\log_2(l)+10$ | $360\ l^3$ | $(\pi\ 2^l)^{1/2}$ |
| 110 | 657,47 | $0{,}48\cdot10^9$ | $6{,}39\cdot10^{16}$ |
| 163 | 941,84 | $1{,}56\cdot10^9$ | $6{,}06\cdot10^{24}$ |
| 224 | 1256 | $4{,}05\cdot10^9$ | $9{,}20\cdot10^{33}$ |
| 256 | 1434 | $6{,}04\cdot10^9$ | $6{,}03\cdot10^{38}$ |
| 512 | 2769 | $48{,}32\cdot10^9$ | $2{,}05\cdot10^{77}$ |

Таблиця 2

Потрібні ресурси для факторизації

| Квантовий комп'ютер | | | Класичний комп'ютер |
|---|---|---|---|
| Квантовий алгоритм факторизації модифікація алгоритму Шора | | | Загальний метод решета числового поля (GNFS) |
| довжина ключа, біт | розмір регістру, кубіт | кількість квантових операцій | кількість класичних операцій |
| $l$ | $2\ l$ | $4\ l^3$ | $L_n[1/3;(64/9)^{1/3}]$ |
| 512 | 1024 | $0{,}54\cdot10^9$ | $2{,}96\cdot10^{11}$ |
| 1024 | 2048 | $4{,}3\cdot10^9$ | $5{,}61\cdot10^{15}$ |
| 2048 | 4096 | $34\cdot10^9$ | $2{,}58\cdot10^{21}$ |
| 3072 | 6144 | $120\cdot10^9$ | $3{,}40\cdot10^{25}$ |
| 15360 | 30720 | $1{,}5\cdot10^{13}$ | $1{,}87\cdot10^{50}$ |

Порівняння табл. 1 та 2 свідчить про те, що для еквівалентних по складності для класичного комп'ютеру задач факторизації та ECDLP, квантове рішення задачі ECDLP потребує менших ресурсів (як кількості кубітів, так й квантового часу), у порівнянні з рішенням задачі факторизації. Різниця об'ємів потрібних ресурсів зростає в залежності від збільшення класичної складності.

Детальна оцінка стійкості симетричних систем проти квантового алгоритму Гровера наведена в приведена в табл. 3 [13].

**Оцінка наявних ресурсів сучасних та перспективних квантових комп'ютерів.**

Основною перешкодою при побудови квантового комп'ютеру є складність побудови квантового регістру з достатньою кількістю кубітів та прийнятної якості.

Канадська компанія D-Wave Systems ще з 2007 року заявляла про створення різних варіантів квантового комп'ютеру D-Wave: Orion з 28 кубітами у 2007 році; One зі 128 кубітами у 2011 році; Vesuvius з 512 кубітами у 2012 році; з більш ніж 1000 кубітами у 2015 році [21]. Але, як показує аналіз, комп'ютер D-Wave для обчислень використовує зовсім інший принцип – так зване адіабатичне квантове обчислення.

Це значно обмежує його можливості, але дозволяє не турбуватися про декогеренції та інші проблеми, що характерні для звичайних квантових обчислень. Тобто вважається, що ні алгоритм Шора, ні алгоритм Гровера на комп'ютері D-Wave не можуть бути реалізовані [22]. У 2015 році фахівці компанії Google підтвердили, що згідно з їх дослідженнями комп'ютер D-Wave використовує квантові ефекти, однак при цьому в "1000-кубітному" комп'ютері кубіти в дійсності організовані лише в кластери по 8 кубітів кожний.

Таблиця 3

Стійкість симетричних криптосистем

| Шифр | Розмір блока /ключа, біт | Кількість необхідної пам'яті для атаки на блок повідомлення/ключ, кубіт | Стійкість при атаці на | |
|---|---|---|---|---|
| | | | блок повідомлення | ключ |
| AES-128 | 128/128 | 128/128 | $2^{64}$ ($10^{19,2}$) | $2^{64}$ ($10^{19,2}$) |
| AES-256 | 128/256 | 128/256 | $2^{64}$ ($10^{19,2}$) | $2^{128}$ ($10^{38,4}$) |
| DES | 64/56 | 64/56 | $2^{32}$ ($10^{9,6}$) | $2^{28}$ ($10^{8,4}$) |
| TDES | 64/168 | 64/168 | $2^{32}$ ($10^{9,6}$) | $2^{134}$ ($10^{40,2}$) |
| ГОСТ-28147 | 64/256 | 64/256 | $2^{32}$ ($10^{9,6}$) | $2^{128}$ ($10^{38,4}$) |
| Калина-128 | 128/128 | 128/128 | $2^{64}$ ($10^{19,2}$) | $2^{64}$ ($10^{19,2}$) |
| Калина-256 | 256/256 | 256/256 | $2^{128}$ ($10^{38,4}$) | $2^{128}$ ($10^{38,4}$) |
| Калина-512 | 512/512 | 512/512 | $2^{256}$ ($10^{76,8}$) | $2^{256}$ ($10^{76,8}$) |
| Blowfish | 64/448 | 64/448 | $2^{32}$ ($10^{9,6}$) | $2^{224}$ ($10^{67,2}$) |

Квантовий комп'ютер з двома кубітами на кристалі алмазу з домішками, який функціонує при кімнатній температурі і теоретично є масштабованим у квітні 2012 року створила група дослідників з Південно-Каліфорнійського університету [23]. На цьому комп'ютері реалізовано алгоритм Гровера для чотирьох варіантів перебору, що дозволило отримати правильну відповідь з першої спроби в 95 % випадків [23].

Квантовий комп'ютер компанії IBM [24] містить п'ять кубістів, з яких чотири використовуються для роботи з даними, а п'ятий для корекції помилок під час обчислень. На ньому працює алгоритм Шора. Вчені IBM стверджують, що їх комп'ютер здатний виявляти та вимірювати два виду квантових помилок одночасно. До 2025 року у IBM планують побудувати квантовий комп'ютер, що буде містить кластер об'ємом від 50 до 100 кубітів.

У жовтні 2015 року дослідники з університету Нового Південного Уэльсу вперше побудували квантовий логічний елемент на кремнії.

У жовтні 2016 року Базельский університет запропонував варіант квантового комп'ютеру, який замість того, щоб маніпулювати електронними спінами використовує електронні дірки в напівпровіднику при низьких температурах, оскільки дірки набагато менш вразливі до декогеренції.

Рекорди квантової факторізації наведено у табл. 6 [25].

Виходячи з табл. 6, можливості квантового криптоаналізу не обмежуються прямим використанням алгоритмів Шора и Гровера. Дуже перспективний алгоритм мінімізації викладений в [25] за допомогою якого з використання всього 6 кубітів факторизовано число 291311.

Також, деякі автори вважають, що існують способи розділення загальної задачі на декілька підзадач (частина яких вирішується на класичному комп'ютері), які потребують меншої кількості кубітів.

**Огляд перспективних напрямків досліджень математичних задач, яки є складними для обчислень з використанням квантових комп'ютерів.**

Стрімкий розвиток досліджень в області створення квантових комп'ютерів примушує шукати в якості основи систем ЕЦП нові задачі, які мають експоненціальну складність при використанні як звичайних, так и квантових комп'ютерів. Квантово-стійкими (quantum-resistant) криптосистемами займається так звана "постквантова криптографія" (PQCrypto). Міжнародні конференції PQCrypto проходили у 2006, 2008, 2010, 2011, 2013, 2014, 2016 роках.

Одним з перших прикладів є ЕЦП Меркла з відкритим ключем на основі хеш-дерева. Ральф Чарльз Меркл запропонував цей алгоритм у 1979 році, як альтернативу ЕЦП RSA та DSA. Основний недолік схеми Меркла полягає в тому, що для будь-якого відкритого ключа на основі хеш-функції існує обмеження на кількість підписів, яки можуть бути отримані з відповідного набора закритих ключів.

Автор [32] вважає, що є чотири основних напрямки постквантової криптографії: дослідження задач теорії алгебраїчних решіток; дослідження теорії кодування; вивчення багатоваріантних квадратичних систем; вивчення некомутативних груп, в число яких входять групи кос.

Першим напрямком є використання теорії решіток, яка була запропонована Германом Минковским (Hermann Minkowski) [33]. В цієї теорії є різні складні задачі [34], які можуть бути використані в PQCrypto в якості примітивів. Найбільш важливими є задачі пошуку найкоротшого (shortest vector problem (SVP)) та найближчого векторів (closest vector problem (CVP)).

Айтай (Ajtai) в роботі [35] показав, що в загальному випадку задача SVP є NP-важкою, однак криптосистем, стійкість яких може бути зведена до рішення цієї задачі, не існує. Однак, стійкість систем Айтая-Дворка (Ajtai-Dwork) [36] та Реджева (Regev) [36] може бути зведена до рішення цієї задачі в підкласі решіток, в яких найкоротший ненульовий вектор є унікальним (unique shortest vector problem, uSVP; пошук унікального найкоротшого вектору).

Miccianclo (Micciancio) [37] доказав, що задача $\gamma$ -SVP є NP-важкою при $\gamma \le \sqrt{2}$. Ван Емде-Бос (Van Emde-Boas) [38] показав, що задача CVP є NP-важкою, а Ерора (Агога) з колегами [39] встановив, що задача $\gamma$ -CVP є NP-важкою при $\gamma = \log(n)^c$ для $c > 0$. Голдвассер (Goldwasser) и Голдрейх (Goldreich) отримали комплексний теоретичний аргумент, що $\gamma$ -CVP не може бути NP-важким для $\gamma = \Omega\left(\sqrt{n} / \log(n)\right)$. Більш

докладно ці докази розглянуті в [40].

Стійкість криптосистем NTRUEncrypt (які раніше мали назву NTRU) також основана на SVP [41]. Співвідношення для оцінки складності атак на систему NTRU наведено у табл. 4 [42].

Таблиця 4

Часова та просторова складність атак на NTRU

| Складність | |
|---|---|
| часова | просторова |
| Атака методом грубої сили | |
| $O\left(C_N^d\right)$ | O(1) |
| Класична атака зустріч посередині | |
| $O\left(C_{N/2}^{d/2}/\sqrt{N}\right)$ | $O\left(C_{N/2}^{d/2}/\sqrt{N}\right)$ |
| Атака методом Ванга | |
| $O\left(\sqrt{C_{N+1}^d}\right)$ | O(1) |
| Квантова атака зустріч посередині (метод Ксіонга) | |
| $O\left(C_{N/2}^{d/2}\cdot\log\left(C_{N/2}^{d/2}\right)\right)+\bar{O}\left(\sqrt{C_{N/2+1}^{d/2}}\right)$ | $O\left(C_{N/2}^{d/2}\right)$ |
| Удосконалена квантова атака зустріч посередині (метод Ванга) | |
| $O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\cdot\log\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)\right)+\bar{O}\left(\sqrt{C_{N-\lfloor N/3\rfloor+1}^{d-\lfloor d/3\rfloor}}\right)$ | $O\left(C_{\lfloor N/3\rfloor}^{\lfloor d/3\rfloor}\right)$ |

Порівняльний аналіз часової складності для різних розмірів системних параметрів NTRU та різних атак наведено у табл. 5 [13].

З аналізу табл. 5 видно, що система NTRUEncrypt є вразливою до удосконаленої квантової атаки зустріч посередині (метод Ванга).

**Другим напрямком** пошуку задач, які є складними для обчислення на квантових комп'ютерах, є задачі теорії кодів з виправленням помилок. Однією з них є задача декодування. Використовують для шифрування лінійні коди, наприклад, в криптосистемах МакЕліса (McElece) [43] та Нідеррейтера (Niederreiter) [44]. Для зашифрування повідомлення здійснюють його кодування і додають вектор помилок з заданим ваговим коефіцієнтом t. Розшифрування потребує рішення задачі декодування.

Використання таких систем обмежується наступними вимогами. Задача декодування повинна мати ефективне рішення для ефективної корекції помилок.

Крім того, криптосистеми, що засновані на теорії кодів, є стійкими тільки у тому випадку, якщо задача декодування стає обчислювально складною в умовах невідомого секрету, що вірно і для двійкових кодів Гоппи (Goppa).

Розшифрування криптосистем, що засновані на теорії кодів, означає рішення задачі декодування, в якій відомий ваговий коефіцієнт вектору помилок. Якщо не маємо додаткової інформації про лінійний код, наприклад, про породжуючий багаточлен коду Гоппи, то можемо використовувати лише базові методи декодування. Зламування таких криптосистем потребує рішення задачі криптографічного декодування.

Таблиця 5

Часова складність різних алгоритмів криптоаналізу NTRU

| Параметри NTRU | | | | |
|---|---|---|---|---|
| NTRU 251 | NTRU 347 | NTRU 491 | NTRU 587 | NTRU 787 |
| Груба сила | | | | |
| $10^{52}$ | $10^{72}$ | $10^{100}$ | $10^{120}$ | $10^{159}$ |
| Класична атака зустріч посередині | | | | |
| $10^{24}$ | $10^{34}$ | $10^{48}$ | $10^{58}$ | $10^{77}$ |
| Атака методом Ванга | | | | |
| $10^{26}$ | $10^{36}$ | $10^{50}$ | $10^{60}$ | $10^{79}$ |
| Квантова атака зустріч посередині (метод Ксіонга) | | | | |
| $3.3\cdot10^{27}+7\cdot10^{12}$ | $4.6\cdot10^{37}+6.9\cdot10^{17}$ | $3.2\cdot10^{52}+1.5\cdot10^{25}$ | $4.5\cdot10^{60}+7.6\cdot10^{29}$ | $1.5\cdot10^{81}+2.7\cdot10^{39}$ |
| Удосконалена квантова атака зустріч посередині (метод Ванга) | | | | |
| $3.5\cdot10^{18}+1.6\cdot10^{17}$ | $9\cdot10^{25}+7.6\cdot10^{23}$ | $3\cdot10^{35}+1.8\cdot10^{33}$ | $3.8\cdot10^{41}+9\ 10^{39}$ | $4.6\ 10^{54}+3.7\ 10^{52}$ |

Таблиця 6

Рекорди квантової факторизації

| Число що факторизувалось | Число кубіт | Алгоритм | Рік та посилання |
|---|---|---|---|
| 15 | 8 | Шора | 2001 [26] |
| 15 | 8 | Шора | 2007 [27] |
| 15 | 8 | Шора | 2009 [28] |
| 15 | 8 | Шора | 2012 [29] |
| 21 | 10 | Шора | 2012 [30] |
| 143 | 4 | Мінімізації | 2012 [31] |
| 56153 | 4 | Мінімізації | 2012 [31] |
| 291311 | 6 | Мінімізації | 2012 [31] |

Криптосистема Нідеррайтера дозволяє створювати ЕЦП. Незважаючи на те, що ця криптосистема була зламана, деякі її модифікації залишаються кріпостійкими [57].

**Третім напрямком** пошуку задач, які є складними для обчислення на квантових комп'ютерах, є задачі вирішення системи квадратних рівнянь з декількома змінними, що задані над кінцевим полем. У [46] вказано, що, в загальному випадку, ця задача є NP-повною.

Стандартний метод рішення таких задач містить в собі знаходження базису Гребнера, яке навіть з використанням кращих алгоритмів займає час, який експоненціально збільшується в залежності від розміру вихідних даних. Варіант побудови такої системи розглянутий в роботі [45]. Криптографічні системи, побудовані з використанням вищезазначеного методу, отримали назву HFE-систем (Hidden Field Equations, замаскована система рівнянь над полем). В роботі [45] наводяться додаткові методи

рішення цієї задачі та показано, що питання точної оцінки часу рішення цієї задачі залишається відкритим та потребує додаткових досліджень.

Відомі дві атаки на HFE- систему:

– визначення секретного ключа (Shamir-Kipnis). Основним моментом цієї атаки є визначення секретного ключа за допомогою розріджених одноваріантних багаточленів над полем розширення $F_{q^n}$. Атака ефективна не для всіх варіацій HFE;

– швидке обчислення базису Гребнера (Faugere). Ідея атак Faugere полягає в використанні швидкого алгоритму для обчислення базису Гребнера системи поліноміальних рівнянь.

**Четвертим та найбільш перспективним** напрямком пошуку криптографічних примітивів, які є стійкими до атак з використанням квантових комп'ютерів, є дослідження в області побудови схем з відкритим ключем, які використовують некомутативні групи.

Перша та невдала спроба використати некомутативні групи була здійснена Емілем Артіном (Emil Artin) в роботі [47]. Він запропонував використання груп кос в якості криптографічного примітиву.

Задача визначення рівняння двох кос (word problem), що задані композицією генераторів, ефективно вирішується, як показано в роботі [48].

Задача пошуку спряжень (Conjugacy Search Problem, CSP) та її варіації являє собою відправну точку в побудові однонаправлених функцій.

Цю задачу можливо модифікувати двома способами, указав додаткові умови:

– елемент, що спрягається, належить до визначеної підгрупи групи (Generalized Conjugacy Search Problem, GCSP);

– декілька заданих пар кос спрягаються одним елементом (Multiple Conjugacy Search Problem, MCSP).

Крім того, можна використати більш просту задачу Braid Diffie-Hellman Problem (BDHP).

Однак з'явились декілька ефективних методів атаки на CSP.

Метод "Summit Sets". Сутність цього методу полягає у визначенні виділеної підмножини всіх спряжень заданого елементу групи, яке може бути ефективно обчислено. Даний метод був описаний в роботі [49] Гарсайда (Garside) та пізніше уточнений Ель-Ріфаі (El-Rifai) та Мортоном (Morton) в [50], а також Гебхардтом (Gebhardt) в [51]. Гебхардт (Gebhardt) у роботі [51] повідомляє, що задача CSP с косами, які мають довжину порядку 1000, з використанням цього методу, вирішується менш ніж за хвилину часу обчислень.

Метод лінійних представлень, що використовується в роботі [52], забезпечує рішення задачі BDHP за час, який поліноміально залежить від числа нитей в косах n та від їх довжини *l*.

В [53] зазначено, що використання в якості примітива для побудови криптографічних протоколів задачі CSP не забезпечує потрібного рівня складності. В роботі [54] було запропоновано розширити задачі, що застосовуються до груп кос, для кінцевих некомутативних груп.

Одним з найбільш перспективних напрямків пошуку криптографічних примітивів, стійких до атак з використанням квантових комп'ютерів, є дослідження в області побудови схем з відкритим ключем, що використовують так звану задачу дискретного логарифмування в скритій підгрупі некомутативної групи.

Найбільш поширеною в науковій літературі криптографічною схемою, яка побудована на основі цієї задачі, є криптографічна схема MOR [55].

Як показано в роботі [54], в якості некомутативних кінцевих груп також можуть бути використані кінцеві групи матриць та кінцеві групи векторів, що мають непарні значення розмірності. Групи векторів такого типу задаються за допомогою завдання операції множення векторів, які мають властивості асоціативності та некомутативності. Варіанти таких груп розглянуті в [56].

## Висновки

Проведений огляд літератури показав, що алгоритми Шора та Гровера для квантових комп'ютерів мають поліноміальну залежність часу виконання від довжини ключа. Відомі алгоритми для класичних комп'ютерів в кращому випадку мають субекспоненціальну залежність. Це визвало значний інтерес к дослідженням в області квантових алгоритмів і розробці квантових комп'ютерів. Однак, на теперішній час не створені квантові комп'ютери з числом повноцінних кубітів, що дорівнює довжині сучасних ключів. Але такі комп'ютери будуть створені.

У зв'язку з цим, актуальними є дослідження, які направлені на розробку криптографічних систем, що будуть стійкими до атак з використанням таких комп'ютерів.

Необхідною умовою для існування постквантових систем ЕЦП є наявність важкої обчислювальної задачі, яку неможливо вирішити за прийнятний час, як на квантовому, так й на класичному комп'ютері, та яка може бути використана в якості теоретичного примітиву при побудові таких систем. На сьогоднішній день є декілька напрямків постквантової криптографії – дослідження задач теорії алгебраїчних решіток, теорії кодування, некомутативних груп векторів (матриць), а також багатоваріантних квадратичних систем.

Криптосистеми NTRU на базі теорії алгебраїчних решіток можуть стати уразливими до квантового криптоаналізу, хоча ще не так давно зазначалося,

що такі схеми будуть стійкі проти нього.

Одним з найбільш перспективних напрямків є дослідження в області побудови схем з відкритим ключем, які використовують так звану задачу дискретного логарифмування в скритій підгрупі некомутативної групи.

## Список літератури


*1. Deutsch D. Rapid Solution of problems by quantum computation [Text] / D. Deutsch, R. Jozsa // Proc. R. Soc. Lond. A. – 1992. – Vol. 439 (1907). – P. 553-558.*

*2. FIPS-186-3. Digital signature standard: 2009 [Text]. 2009 – 07 – 19 - Gaithersburg, MD20899-8900 - 2009 – 120 p.*

*3. 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.*

*4. Shor Peter W. Algorithms for quantum computer: Discrete logarithms and factoring / Peter W. Shor. – 1994.*

*5. 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). – P. 1484-1509.*

*6. Volovich I.V. Quantum computing and Shor's factoring algorithm. arXiv.quantph/0109004 v1, 2001.*

*7. John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv.quantph/0301141 v2, 2004.*

*8. Лов К. Гровер. Квантовая механика помогает найти иголку в стоге сена. [Text] / Лов К. Гровер // Phys. Rev. Lett., 79(2) – 1997. – P. 325-328.*

*9. Lenstra A.K. and Jr. (Eds.) Lenstra H.W. The developement of the number field sieve. Springer-Verlag, 1993.*

*10. Lenstra A.K. and Verheul E.R. Selecting cryptographic key sizes, 1999.*

*11. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003.*

*12. Кнут Дональд Эрвин. Искусство программирования, том 2. Получисленные алгоритмы, 3-е изд. / Дональд Эрвин Кнут. – М.: Издательский дом «Вильямс», 2000.*

*13. 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. – 1/9 (67), 2014. – С. 8-16, ISSN 1729-3774.*

*14. Богданов А.Ю. Квантовые алгоритмы и их влияние на безопасность современных классических криптографических систем. [Electronic resource] / /А.Ю. Богданов, И.С. Кижватов // РГГУ. – 2005. – 18 с. Режим доступу: \www/ URL: – http://crypto.rsuh.ru/papers/bogdanov-kizhvatov-quantum.pdf.*

*15. Гайнутдинова А.Ф. Квантовые вычисления [Текст]: метод. пособ. / А.Ф. Гайнутдинова. – Казань: Казанский государственный университет, 2009. – 272 с.*

*16. Menezes Alfred J. Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – CRC Press, 1996. ISBN 0-8493-8523-7.*

*17. Coppersmith D. Discrete logarithms in GF(p) / D. Coppersmith, A. Odlyzko, R. Schroeppel // Algorithmica. – 1986. – V. 1. – P. 1-15.*

*18. Schirokauer O. Discrete logarithms and local units / O. Schirokauer // Phil. Trans. R. Soc. Lond. A., V. 345, 1993. – P. 409-423.*

*19. Adleman L. A Subexponential Algorithm for the Discrete Logarithm with Application to Cryptography / L. Adleman // Proceedings of the IEEE 20th Annual Symposium on Foundations of Computer Science (FOCS), 1979. – P. 55-60.*

*20. Analysis of the xedni-calculus attack / M. Jacobson, N. Koblitz, J. Silverman, A. Stein, Teske. – Preprint 1999.*

*21. D-Wave Systems: official site. [Електронний ресурс]. – Режим доступу: http:// www.dwavesys.com/services.*

*22. Lockheed Martin piece about D-Wave technology [Electronic resource] / Burnaby, British Columbia, Canada Блог компанії D-Wave Режим доступу: \www/ URL: – http://dwave.wordpress.com/2013/03/08/lockheed-martin-piece-about-d-wave-technology/. – 08.03.2013 р.*

*23. Quantum computer built inside diamond [Electronic resource] / Futurity Research news from top universities-Режим доступу: \www/ URL: – http://www.futurity.org/ quantum-computer-built-inside-diamond/ - 09.04.2012.*

*24. Сайт компанії IBM [Electronic resource] / Режим доступу: /www / URL: http://arstechnica.com/science/ 2016/05/how-ibms-new-five-qubit-universal-quantum-computer-works/- 20.05.2016.*

*25. Nikesh S. Dattani, Nathaniel Bryans. "Quantum factorization of 56153 with only 4 qubits" arXiv:quantph/1411.6758v3 27 Nov. 2014.*

*26. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature / L.M. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuangvol. – 414, no. 6866. – P. 883-7, Jan. 2001.*

*27. Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement / B. Lanyon, T. Weinhold, N. Langford, M. Barbieri, D. James, A. Gilchrist, A. White // Physical Review Letters, Dec. – 2007. – Vol. 99, no. 25. – P. 250505.*

*28. Politi A. Shor's quantum factoring algorithm on a photonic chip / A. Politi, J.C.F. Matthews, J.L. O'Brien // Science. – Sep. 2009. – Vol. 325, no. 5945. – P. 1221.*

*29. Experimental realization of Shor's quantum factoring algorithm using qubit recycling / E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, J.L. O'Brien // Nature Photonics. – Oct. 2012. – Vol. 6, no. 11. – P. 773-776.*

*30. Computing prime factors with a Josephson phase qubit quantum processor / E. Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland, J.M. Martinis // Nature Physics. – Aug. 2012. – Vol. 8, no. 10. – P. 719-723.*

*31. Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System / N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng, J. Du // Physical Review Letters. – Mar. 2012. – Vol. 108, no. 13. – P. 130501.*

*32. Buchmann J. Post-Quantum Signatures / Johannes Buchmann, Carlos Coronado, Martin Doring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt, Ulrich Vollmer, Ralf-Philipp Weinmann. – 2004. – P. 3-15.*

*33. Minkowski H. Geometrie der Zahlen / H. Minkowski. – Leipzig: Teubner, 1896. – 256 p.*

*34. Усатюк В.С. Задачи теории решеток и их взаимные редукции [Електронний ресурс] / В.С. Усатюк. – Режим доступу до ресурсу: www/ URL: http://rgupenza.ru/mni /content/files/10_2_Usatjuk.doc.*

*35. Ajtai M. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract) / M. Ajtai // Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing. – ACM Press, 1998. – P. 10-19.*

*35. Ajtai M. A public-key cryptosystem with worstcase /average-case equivalence / M. Ajtai, C Dwork // Proceedings of the 29th Annual Symposium on Theory of Computing (STOC). – ACM Press, 1997. – P. 284-293.*

*36. Regev O. New lattice based cryptographic constructions / Oded Regev // Journal of the ACM. – ACM Press, 2004. – Vol. 51. – P. 899-942.*

*37. Micciancio D. The shortest vector problem is NP-hard to approximate to within some constant / Daniele Micciancio // SIAM Journal on Computing. – 2001. – Vol. 30, no. 6. – P. 2008-2035.*

*38. Van Emde Boas P. Another NP-complete partition problem and the complexity of computing short vectors in a*

*lattice / P. van Emde Boas // Tech. Report 81-04. University of Amsterdam, Department of Mathematics, Netherlands. – 1981.*

*39. Arora S. The hardness of approximate optima in lattices, codes, and systems of linear equations / S. Arora, L. Babai, J. Stern, E.Z. Sweedyk // Journal of Computer and System Sciences. – 54 (1997), no. 2. – P. 317-331.*

*40. Micciancio D. Complexity of lattice problems / D. Micciancio, S. Goldwasser // Kluwer Academic Publishers. – 2002.*

*41. 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.*

*42. 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. – P. 3514-3518.*

*43. McEliece R.J. A public key cryptosystem based on algebraic coding theory / R.J. McEliece // DSN progress report 42-44. – 1978. – P. 114-116.*

*44. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory / H. Niederreiter // Problems of Control and Information Theory. – 1986. – Vol. 15, no. 2. – P. 159-166.*

*45. Buchmann J. Post-Quantum Signatures / Johannes Buchmann, Carlos Coronado, Martin Doring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt, Ulrich Vollmer, Ralf-Philipp Weinmann. – 2004. – P. 3-15.*

*46. Garey M.R. Computers and Intractability - A Guide to the Theory of NPCompleteness / M.R. Garey, D.S. Johnson. – W. H. Freeman and Company, 1979.*

*47. Artin E. Theorie der Zopfe / E. Artin // Hamburg Abh. – 1925. – Vol. 4. – P. 47-72.*

*48. Choon Cha J. An efficient implementation of braid groups / Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, Jung Hee Cheon // Lecture Notes in Computer Science. – Springer, 2001. – Vol. 2248. – P. 144-156.*

*49. Garside F.A. The braid group and other groups / F.A. Garside // Quarterly Jounal of Mathematics Oxford Series. – 1969. – Vol. 20, no. 2. – P. 235-254.*

*50. El-Rifai E.A. Algorithms for positive braids / E.A. El-Rifai, H.R. Morton // Quarterly Jounal of Mathematics Oxford Series. – 1994. – Vol. 45, no. 2. – P. 479-497.*

*51. Gebhardt V. A new approach to the conjuagacy problem in garside groups / V. Gebhardt // Journal of Algebra. – 2005. – Vol. 292. – P. 282-302.*

*52. Hee Cheon J. A polynomial time algorithm for the braid diffie-hellman conjugacy problem / Jung Hee Cheon, Byungheup Jun. // Lecture Notes in Computer Science. – Springer, 2003. – Vol. 2729. – P. 212-225.*

*53. Myasnikov A. A Practical Attack on a Braid Group Based Cryptographic Protocol / A. Myasnikov, V. Shpilrain, A. Ushakov // Lecture Notes in Computer Science. – Springer, 2005. – Vol. 3621. – P. 86-96.*

*54. Moldovyan D.N. A New Hard Problem over Non-Commutative Finite Groups for Cryptographic Protocols / D.N. Moldovyan, N.A. Moldovyan // Lecture Notes in Computer Science. – Springer, 2010. – Vol. 6258. – P. 183-194.*

*55. Seong-Hun Paeng. New public key cryptosystem using finite non-abelian groups / Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, Choonsik Park // Lecture Notes in Computer Science. – Springer, 2001. – Vol. 2139. – P. 470-485.*

*56. Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи / Д.Н. Молдовян, И.А. Куприянов, А.А. Костина, Д.В. Захаров // Вопросы защиты информации. – 2009. – № 4. – С. 12-18.*

*57. Самохина М.А. Модификации криптосистемы Нидеррайтера, их стойкость и практические применения / М.А. Самохина // Труды МФТИ. – М.: 2009. – Т. 1, вып. 2. – С. 121-127. – ISSN 2072-6759.*

*Надійшла до редколегії 30.09.2016*

**Рецензент:** д-р техн. наук, ст. наук. співробітн. В.О. Василець, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

## ОБЗОР ВОЗМОЖНОСТЕЙ КВАНТОВОГО КРИПТОАНАЛИЗА И КРИПТОГРАФИЧЕСКИХ ПЛАТФОРМ, КОТОРЫЕ ЯВЛЯЮТСЯ СТОЙКИМИ К НЕМУ И МОГУТ БЫТЬ ОСНОВОЙ ДЛЯ СИСТЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.С. Бурковский

*Представлена сравнительная оценка сложности алгоритмов криптоанализа на квантовом и классическом компьютере. Рассматриваются криптографические платформы, которые являются стойкими к квантовому криптоанализу и могут быть основой для систем электронной цифровой подписи.*

***Ключевые слова:*** *алгоритм квантовый, алгоритм Шора, алгоритм Гровера, электронная цифровая подпись, постквантовая криптографическая платформа.*

## REVIEW OF POSSIBILITIES OF QUANTUM CRYPTOANALYSIS AND CRYPTOGRAPHIC PLATFORMS, WHICH ARE PROOF TO HIM AND CAN BE BASIS FOR THE SYSTEMS OF ELECTRONIC DIGITAL SIGNATURE

V.S. Burkovskiy

*The comparative estimation of complication of algorithms of cryptoanalysis is presented on a quantum and classic computer. Cryptographic platforms which are proof to quantum cryptoanalysis and can be basis for the systems of electronic digital signature are examined.*

***Keywords:*** *an algorithm is a quantum, algorithm Shora, algorithm of Grovera, electronic digital signature, postquantum cryptographic platform.*