ПРОБЛЕМЫ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ И ВОЗМОЖНЫЕ НАПРАВЛЕНИЯ ИХ РАЗРЕШЕНИЯ В БУДУЩЕМ

УДК 004.056.55

І.Д. ГОРБЕНКО, д-р техн. наук, О.О. КУЗНЄЦОВ, д-р техн. наук,
О.В. ПОТІЙ, д-р техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук, Р. С. ГАНЗЯ,
В.А. ПОНОМАР

ПОСТКВАНТОВА КРИПТОГРАФІЯ ТА МЕХАНІЗМИ ЇЇ РЕАЛІЗАЦІЇ

Вступ

В 2012 – 2015 рр. зроблено суттєві кроки відносно побудови квантового комп'ютера [1 – 4]. В певній мірі розроблені та чекають свого часу методи та алгоритми квантового криптоаналізу. Такі досягнення викликали необхідність більш детальних оцінок криптографічної стійкості існуючих криптоперетворень та криптосистем, прогнозування їх стійкості в постквантовий період. Практичні висновки таких досліджень викликали стурбованість на самому високому світовому рівні. Так, в Інтернеті 01.11.2015 р. опублікована стаття «A RIDDLE WRAPPED IN AN ENIGMA [1], автори якої – видатні криптологи США – професори Ніл Кобліц та Альфред Менезес. В ній відмічається, що в серпні 2015 р. агентство національної безпеки (АНБ) уряду США виступило з заявою про слабкість існуючих криптосистем відносно методів квантового криптоаналізу та необхідність розробки постквантових стандартів криптографічного захисту інформації. Подальшим підтвердженням стурбованості уряду США відносно необхідності розробки нових стандартів криптографічного захисту інформації є опублікування звіту «Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT)» [2], в якому повністю підтверджено вказані вище загрози. Більш того, в цьому звіті визначено основні проблеми та можливості і етапи їх вирішеня.

Зважаючи на проблемність та необхідність розв'язання задач криптоаналізу нині діючих стандартизованих криптографічних перетворень, тобто оцінки їх стійкості у постквантовий період, особлива увага нині зосереджена на визначенні можливостей розв'язання задач криптоаналізу з використанням квантових комп'ютерів та, в першу чергу, розроблення відповідних методів та алгоритмів квантового криптоаналізу. Таким чином, у світі вирішуються дві проблеми – створення квантового комп'ютера та розробка і реалізація математичних методів квантового криптоаналізу.

Скоріше всього, у випадку появи квантового комп'ютера, що може реалізувати уже розроблені квантові алгоритми, зокрема алгоритми криптоаналізу Шора [3, 5, 7, 9] та Гровера [3, 6, 10, 13, 14], Ксіонга та Ванга та Ксіонга [3, 15, 16], можуть виникнути великі загрози у інформаційній сфері відносно забезпечення криптографічної стійкості для існуючих асиметричних криптоперетворень. При цьому важливим є не тільки сам факт побудови такого комп'ютера, а й його технічні характеристики. Вказане необхідно враховувати, так як існуючі квантові алгоритми для своєї «роботи» потребують значних технічних ресурсів, особливо просторових у вигляді кількості кубітів регістрів [1 – 6, 18 – 20].

У грудні 2015 року фахівці компанії Google підтвердили, що згідно з їх дослідженням в комп'ютері D-Wave використовуються квантові ефекти. При цьому в «1000-кубітном» комп'ютері кубіти в дійсності організовані в кластери по 8 кубіт кожен. Якраз це і дозволило добитися в одному з алгоритмів [21] швидкодії в 100 млн разів більше ніж у звичайному комп'ютері.

Сьогодні в криптології існує ряд проблемних задач повного розкриття [3]. Детальний аналіз дозволив виділити основні методи криптоаналізу для застосування на квантовому комп'ютері (звичайно, якщо він буде побудований з відповідними характеристиками). До

основних задач, які можуть бути вирішені на квантовому комп'ютері, необхідно віднести такі [4 – 17]:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гроувера;
- квантовий алгоритм Шора розв'язку дискретного логарифму в скінченному полі;
- квантовий алгоритм розв'язку дискретного логарифму в групі точок еліптичної кривої Шора;
- квантовий алгоритм криптоаналізу для перетворень в фактор-кільці;
- квантовий алгоритм криптоаналізу Ксіонга та Ванга та його вдосконалення тощо.

Зрозуміло, що вирішення названих проблем потребує часу. Але уже сьогодні необхідно обґрунтовувати та розробляти моделі порушників постквантового періоду та моделі загроз. Перші спроби вирішення цих задач наведені в [3]. Також, на наш погляд, зважаючи на широке розповсюдження та застосування, в першу чергу необхідно вести дослідження з обгрунтування вимог, визначення основних механізмів постквантових електронних підписів (ЕП) та їх первинного аналізу за критеріями стійкості та складності.

Метою статі є розробка основних положень моделі порушника та загроз у постквантовий період, обгрунтування вимог криптографічних перетворень взагалі та до ЕП зокрема, при виконанні яких вони можуть бути стійкими у постквантовий період, а також визначення основних методів, з використанням яких можуть бути побудовані та стандартизовані міжнародні та національні ЕП.

1. Аналіз основних проблем створення квантового комп'ютера та розробки математичного забезпечення

1.1. Аналіз досягнень в побудові квантового комп'ютера.

Як зазначено вище, на сьогодні вирішуються дві важливі проблеми – створення квантового комп'ютера та розробка і реалізація математичних методів квантового криптоаналізу. Проведемо аналіз стану їх вирішення та відповідних пропозицій.

Основна проблема у побудові квантового комп'ютера полягає в тому, що необхідно створити систему, яка б задовольняла майже несумісним таким вимогам [3 – 20]:

- кубіти (елементи квантового комп'ютера) мають бути максимально ізольовані один від одного та від навколишнього середовища;
- можливість корельованого впливу на пару кубітів, тобто потрібно не тільки вміти змінювати стан одного кубіту, але й ще вмикати та вимикати взаємодію між парою сусідніх кубітів;
- система кубітів має бути досить стабільною, щоб зберігати корельованість станів, але одночасно й легко відновлюваною для нового циклу обчислень;
- реалізовувати таку сукупність зворотних перетворень над системою кубітів, які б дозволили виконати будь-яку логічну операцію;
- під час обчислень система повинна зберігати квантові властивості, але наприкінці треба зробити вимірювання, яке б однозначно визначило стан системи і у такий спосіб звело б квантову інформацію в класичну.

Важливою властивістю квантових об'єктів є можливість здійснювати паралельні операції. Так, для системи із N кубітів, що перебуває в переплутаному стані, ефективно кодується відразу 2N чисел. Тому операція над нею, завдяки когерентності станів різних кубітів, впливає на всі доданки в сумі і це дозволяє обробляти відразу всі 2N чисел.

Існують квантові алгоритми, які надають можливість проводити атаки на такі асиметричні криптосистеми [5 – 13]:

- системи, що базуються на складності факторизації великого цілого числа (RSA);
- системи, що базуються на складності вирішення дискретного логарифму в скінченному полі Галуа (DSA);

– системи, що базуються на складності вирішення дискретного логарифму в групі точок еліптичної кривої (ECC);

– системи на базі алгебраїчних решіток (NTRU).

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.

Значних здобутків досягла фірма D-Wave, яка стала першою компанією, що продала комерційну версію квантового комп'ютера [22]. Так, з 20 травня 2011 р. 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 р. Lockheed Martin підписала багаторічний контракт з D-Wave Systems, що стосується виконання складних обчислювальних завдань на квантових процесорах. Контракт також включає технічне обслуговування, супутні послуги і купівлю квантового комп'ютера D-Wave One.

Квантовий комп'ютер – це пристрій, процеси обчислень та передачі даних у якому грунтуються на явищі квантової суперпозиції і квантової заплутаності. На нинішній час повноцінний квантовий комп'ютер є ще гіпотетичним пристроєм, можливість побудови якого пов'язана з вирішенням складних теоретичних та практичних проблем квантової фізики та складних експериментів. Дослідження в цьому напрямку знаходяться на передньому краї сучасної фізики. Важливою проблемою є обгрунтування вимог та створення мови програмування для квантового комп'ютера.

Відносно поняття «квантовий паралелізм» в обчисленні можна трактувати так: «Дані в процесі обчислень є квантовою інформацією, яка після закінчення процесу перетворюється в класичну шляхом вимірювання кінцевого стану квантового регістра з заданим числом кубітів. При цьому виграш в квантових алгоритмах досягається за рахунок того, що при застосуванні однієї квантової операції велике число коефіцієнтів суперпозиції квантових станів, які у віртуальній формі містять класичну інформацію, перетворюється одночасно».

Вчені D-Wave опублікували статтю, в якій повідомляється, що за допомогою методу кубіто-тунельної спектроскопії ними було доведено наявність квантової когерентності і заплутаності між окремими підгрупами кубітів в процесорі під час проведення обчислень (розміром 2 і 8 елементів).

В той же час програмна заява NIST або АНБ ретельно опрацьована протягом значного часу [1 – 2]. Комітет, відповідальний за її складання, обговорює кожне речення; нічого не залишено на волю випадку або недбалого редагування. Крім того, коли попросили роз'яснити звіт в серпні 2015 р., АНБ випустило оновлену версію, яка значно не відрізняється від першої. Таким чином, ми повинні почати з передумови, що АНБ мало намір в заяві передати, що воно і зробило.

Ще незрозуміло, коли масштабовані квантові комп'ютери будуть доступні, проте в 2015 р. дослідники, що працюють на побудову квантового комп'ютера, підрахували, що цілком ймовірно, що квантовий комп'ютер, здатний атакувати RSA-2048 в лічині години, може бути побудований до 2030 р., але це вимагає закласти в бюджет близько мільярда доларів. Це серйозна довгострокова загроза для криптосистеми, що в даний час стандартизована в NIST. Таким чином, перехід від 112 до 128 біт безпеки, можливо, менш актуальний, ніж перехід від існуючих криптосистем з постквантової криптосистемою. Цей постквантовий перехід викликає багато фундаментальних проблем.

Так, розробка стандартів для постквантової криптографії вимагає значних ресурсів для аналізу кандидата квантово-стійких схем і потребує значного залучення громадськості, щоб забезпечити довіру до алгоритмів NIST. Інтерес в областях квантових обчислень і квантової криптографії останнім часом збільшився в зв'язку з розвитком квантової обчислювальної техніки, і останні зміни NIST це підтверджують [2]. Це дає можливість для взаємодії з науковою спільнотою, що є дійсно неминучим. Отже, NIST починає готуватися до переходу до квантово-стійкої криптографії.

NIST США робить кроки, щоб ініціювати стандартизацію постквантової криптографії. У NIST планується вказати попередні критерії оцінки для квантово-наполегливих стандартів шифрування з відкритим ключем. Критерії включають безпеку та експлуатаційні вимоги. Проект критеріїв буде винесено на обговорення громадськості в 2016 р., ці обговорення мають завершитись до кінця року. У той час NIST почне приймати пропозиції щодо квантово-стійкої асиметричної криптографії, в першу чергу ЕП. NIST буде встановлювати останній термін подачі заявок в кінці 2017 р.

Хоча цей процес буде мати багато спільного з процесами, які привели до стандартизації AES і SHA-3 [3], це не змагання. NIST бачить свою роль в управлінні процесом досягнення консенсусу спільноти прозоро і своєчасно. В ідеалі кілька алгоритмів будуть з'являтися за «правильністю вибору». NIST може вибрати один або більше з ЕП, що пройдуть випробовування [20 – 21].

Коли стандарти для квантово-стійкої криптографії з відкритим ключем стануть доступні для аналізу, NIST буде переглядати загрози квантових комп'ютерів до існуючих стандартів та може відкликати такі стандарти. Тому установи повинні бути готові до переходу від існуючих алгоритмів до стійких у постквантовий період вже в найближчі 6 – 8 років. Як показує аналіз, таких стандартизованих ЕП в даний час не існує.

Наведені результати аналізу стану розробки та можливості застосування квантового комп’ютера з урахуванням [1, 2] дозволяють обґрунтувати необхідність та важливість розробки постквантової криптографії. Вирішення цієї задачі можливо при наявності моделі порушника, по суті вона зводиться до моделі квантового комп'ютера з конкретними характеристиками та можливостями реалізації квантових алгоритмів криптоаналізу.

1.2. Аналіз основних загроз відносно криптографічних перетворень у постквантовий період

При побудові моделей загроз у постквантовий період, за нинішніх умов, в якості основних необхідно брати методи криптоаналізу як основні моделі загроз, що можуть бути реалізованими на квантовому комп’ютері при вирішенні задач криптоаналізу. Причому, усі вказані методи повинні бути орієнтовані на використання специфіки квантового комп’ютера та мову програмування на ньому.

До основних задач, які можуть бути вирішені на квантовому комп’ютері, в першу чергу необхідно віднести такі:

квантовий алгоритм факторизації Шора [3, 4, 5];

квантовий алгоритм Гровера [3, 6, 7, 10];

квантовий алгоритм Шора вирішення дискретного логарифму в скінченному полі [3, 11];

квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої [3, 5, 9, 11,13];

квантовий алгоритм криптоаналізу для перетворень в фактор кільці [3, 12, 15 – 18].

Проблема криптоаналізу, на вирішення якої спрямовано метод Гровера, може бути сформульована наступним чином [3, 6, 10]. 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 і, зрозуміло, за менший час. Для пошуку можна скористатися математичним апаратом узагальненого «парадоксу про день народження». Основними умовами застосування цієї моделі є випадковість та рівноймовірність здійснення запитів, тобто вхідних даних. Тому при виконанні k запитів ймовірностей успіху можна оцінити як k/N.

Ця задача може бути вирішена з використанням декількох класичних алгоритмів [8], в яких для підвищення ймовірності успіху процедура повторюється багатократно. Для того щоб при повторюваних квантових перетвореннях отримати результат, що очікується, важливо визначити, коли потрібно зупинитися і провести уточнення [3, 6, 10]. Наприклад, викори-

стовуючи алгоритм Гровера, можна знайти секретний ключ симетричного шифрування чи гешування за $\sqrt{N}$ ітерацій, де N – розмір простору ключів. В якості прикладу в [3] наведено оцінки стійкості симетричних криптографічних систем протиквантового криптоаналізу. Аналіз даних показує, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму Гроувера суттєво зменшується.

Зроблені попередні оцінки показують, що з використанням квантового алгоритму Шора задачу факторизації модуля N можна звести до вирішення еквівалентної проблеми, сутність етапів якої полягає у наступному:

– вибрати випадково й рівномірно ціле число a взаємно просте з N;

– для вибраного числа a, що є взаємно простим з N, знайти порядок r елемента $a \bmod N$.

Взаємну простоту числа та N виконати, використовуючи Алгоритм Евкліда [3, 5]. Якщо a не є взаємно простим з N, то потрібно повторно вибрати a, взаємно просте з N. Якщо a є взаємно простим з N, то порядок r елемента $a \bmod N$ буде дільником числа N.

Збільшення розміру модуля перетворення і відповідно особистого ключа при застосуванні квантового алгоритму Шора не забезпечує необхідного збільшення складності дискретного логарифмування в скінченному полі, як при зломі електронного цифрового підпису, так і направленого шифрування. Наприклад, для модуля $P \geq 2^{3072}$ складність дискретного логарифмування в скінченному полі складає $1.4 \cdot 10^{31}$, а з застосуванням алгоритму Шора – всього $2.9 \cdot 10^{10}$ операцій. В той же час, при застосуванні квантового алгоритму проблемною є реалізація регістрів зі значним числом кубітів – не менше 9216. Досягти такого розміру певний час буде проблемою.

Збільшення розміру порядку базової точки при криптоаналізі з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості криптографічної системи на еліптичних кривих. Також показано [3, 5, 10], що при збільшені модуля складність дискретного логарифмування класичними методами в групі точок еліптичної кривої зі збільшенням порядку базової точки збільшується суттєво. Потрібно взяти до уваги, що реалізація квантового алгоритму пов'язана із застосуванням регістрів з великою кількістю кубітів, яка необхідна для проведення квантової атаки. Наприклад, для базової точки з порядком 2571 необхідно використовувати реєстр з довжиною 4016 кубітів. Вважається, що така велика кількість кубітів певний час буде нереалізуємою.

Комбінуючи атаку зустріч посередині і квантовий алгоритм пошуку Гровера, можна підвищити ефективність атаки посередині на NTRU. Отримані оцінки показують, що часова складність $O(\sqrt{C_{N/2+1}^{d_f/2}})$ різко скоротилася в порівнянні з класичним алгоритмом атаки зустріч посередині $O(\frac{C_{N/2}^{d/2}}{\sqrt{N}})$, з тією ж просторовою складністю. В порівнянні з методом Ванга наведений метод також набагато кращий відносно часової складності. Атака Ванга має майже таку ж складність, як і класична атака зустріч посередині, проте вона має меншу складність відносно просторової складності. Із даних, наведених в [3, табл. 2.15 та 2.16] також видно, що системи на базі NTRU, навіть з використанням параметрів великих розмірів, не забезпечують суттєвої стійкості протиквантової атаки зустріч посередині. У цілому системи на базі NTRU стають уразливі до квантового криптоаналізу. Квантова атака зустріч посередині може нанести велику шкоду системам NTRU у разі появи квантових комп'ютері.

На нинішньому етапі розробки квантового комп'ютера важливо паралельно з вирішенням питань створення апаратних засобів розробити та дослідити математичні методи криптоаналізу з урахуванням вимог та можливостей безпосередньо квантового комп'ютера. Вказані задачі вирішуються уже починаючи з 80-х років XX століття. На нинішній час практично вирішені основні математичні та програмні проблемні питання створення квантового комп'ютера. Частина із вказаних проблемних питань перевірена засобом моделювання на класичних комп'ютерах.

При розробленні моделі загроз у постквантовий період в основу можуть бути покладені такі математичні методи [3 – 17]:

– квантовий алгоритм факторизації Шора;

– квантовий алгоритм Гровера;

– квантовий алгоритм Шора вирішення дискретного логарифму в скінченному полі;

– квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;

– квантові алгоритми Гровера та Ванга криптоаналізу для перетворень в фактор-кільці.

Атака зустріч посередині є найбільш ефективним методом проти NTRU, але часова складність атаки зустріч посередині до цих пір дуже велика. Так, метод Ванга можна розглядати як квантовий пошук «грубої сили», який зменшує часову складність від $O(C_N^{d_f})$ до $O(\sqrt{C_{N+1}^{d_f}})$. Вказане можна використати для комбінації квантових обчислень та атаки зустріч посередині. Такий метод був розроблений та наведений у роботі Ксіонга та Ванга.

Наведені результати аналізу та певних досліджень дозволяють зробити висновок, що на нинішньому етапі основою створення практичних моделей загроз у постквантовий період є розробка їх математичних та програмних основ з урахуванням апаратних практичних можливостей. Їх використання дозволить виконати детальний аналіз постквантових криптографічних примітивів, включаючи ЕП.

2. Вимоги NIST щодо можливих кандидатів постквантових криптопримітивів

NIST розуміє необхідність пошуку нових примітивів, які будуть актуальні у постквантовий період [21]. За планами NIST у 2016 р. здійснюється підготовка до проведення конкурсу на нові постквантові криптографічні стандарти. Вже підготовлений проект вимог до кандидатів. Об'ява конкурсу планується у 2017 р., є сподівання, що до кінця 2019 р. нові стандарті будуть затверджені. Ці роботи здійснюються у рамках відкритого конкурсу Post-Quantum crypto Project. У табл. 1 наведені основні вимоги до кандидатів [21].

Таблиця 1

Вимоги NIST до постквантових криптографічних примітивів

Вимоги з безпеки	
Використання криптографії з відкритим ключем	Заміна стандарту цифрового підпису FIPS 186 Заміна стандартів розподілу ключів SP 800-56A, SP 800-56B Використання нового стандарту в протоколах: TLS, SSH, IPsec, DNSSEC
Модель безпеки для шифрування та розподілу ключів	Схема «семантично безпечного шифрування». Модель безпеки – IND-CCA2. Умови безпеки: доступ зловмисника менше ніж до 2^{64} обраних шифротекстів.
Модель безпеки для електронного підпису	Модель безпеки EUF-CMA. Умови безпеки: доступ зловмисника менше ніж до 2^{64} обраних повідомлень.
Вимоги до стійкості	1) 128 біт класичної безпеки / 64 біт квантової захищеності (запас стійкості AES-128) 2) 128 біт класичної безпеки / 80 біт квантової захищеності (запас стійкості SHA-256/ SHA3-256) 3) 192 біт класичної безпеки / 96 біт квантової захищеності (запас стійкості AES-192) 4) 192 біт класичної безпеки / 128 біт квантової захищеності (запас стійкості SHA-384/ SHA3-384) 5) 256 біт класичної безпеки / 128 біт квантової захищеності (запас стійкості AES-256)

Додаткові властивості безпеки	«perfect forward secrecy» (удосконалена випереджаюча безпека). Стійкість до атак сторонніми каналами. Стійкість до мультиключових атак. Стійкість до відмов.
Інші вимоги	Прозорі математичні рішення при реалізації криптопримітивів. Обґрунтованість стійкості криптоперетворень

Техніко-економічні вимоги

Вимога	Сутність вимоги
Розміри (довжини) відкритого ключа, шифротексту, підпису	Орієнтація на розмір пакетів інтернет-протоколів. Ґешування ключової інформації. Для «perfect forward secrecy» використання менших довжин ключа.
Обчислювальна ефективність операцій відкритого (шифрування перевірки підпису) та особистого ключів (шифрування, підписування)	Забезпечення ефективності як апаратної, так і програмної реалізації.
Обчислювальна ефективність процесу генерування ключів	Відповідність розмірів ключа до обраної системи.
Помилки шифрування	Низький відсоток помилок шифрування. Багаторазове шифрування.
Техніко-експлуатаційні вимоги	
Гнучкість	Додаткові можливості схеми (оптимізація, неявний обмін ключами тощо). Кросплатформеність. Можливість розпаралелювання.
Простота	Зрозумілість та прозорість побудови.

Критерії відбору серед запропонованих кандидатів

Технічна оцінка	
Перевірка на коректність	Перевірка правильності базових та оптимізованих реалізацій.
Перевірка на ефективність	Обчислення часу, необхідного для генерації ключа, шифрування, розшифрування, електронного підпису, перевірки підпису, встановлення ключів, а також розмір ключів, зашифрованого тексту і підпису. (Тестування проводиться на оптимізованих версіях).
Інші перевірки	Додаткові випробування.
Умови випробувань	Основна платформа: NIST PQC Reference Platform, Intel x64, Windows or Linux, the GCC compiler. Також можуть проводитися додаткові тестування за інших умов (8-бітових процесорів, цифрових сигнальних процесорів, виділених CMOS тощо)

Таким чином, у 2016 р. у США розпочалися активні роботи щодо підготовки до проведення конкурсів на майбутніх кандидатів квантово-захищених алгоритмів. Тобто США активно приступили до виконання планів розроблення та прийняття постквантових стандартів криптографічного захисту інформації. Наведені в табл. 1 дані містять вимоги та рекомендації щодо першого етапу розроблення та тестування постквантових примітивів. Вони охоплюють широкий спектр та містять вимоги до безпеки постквантових криптографічних примітивів, техніко-економічні та техніко-експлуатаційні вимоги. Також запропоновано узагальнені критерії оцінки та порівняння можливих кандидатів. На період до прийняття нових стандартів органи стандартизації США уже надали рекомендації стосовно застосування існуючих крип-

тографічних алгоритмів, в першу чергу в частині довжин (розмірів) загальних параметрів та ключів, а також конкретизації криптопримітивів.

В той же час, за нашими дослідженнями, орієнтація на критерій оцінки стійкості з довжиною симетричного ключа 128 біт є недостатньо обгрунтованою. Очевидно потрібно збільшувати довжину блока (при блоковому симетричному перетворенні) і довжину ключа до 256 бітів. Разом з тим, поява наведених вимог є важливим етапом постквантової стандартизації в криптографії.

3. Вимоги до квантово-захищених алгоритмів ЕП ETSI

Європейський Союз також розпочав активну роботу з підготовки нових постквантових стандартів. Зупиняються роботи, пов'язані з виконанням завдань, що були визначені в Регламентах ЄС 2012 та 2014 рр. Європейською організацією зі стандартизації ETSI у кластері «Безпека» сформований новий напрямок «Квантово захищена криптографія» («Quantum-Safe Cryptography») [20, 21].

Крім того, група спеціалістів активно веде дослідження в таких основних напрямках:

– оцінка потенційних загроз безпеці в постквантовий період;

– приклади та сценарії реалізації квантово-захищених примітивів;

– фундаментальні межі можливостей квантових обчислень стосовно існуючих та перспективних криптографічних перетворень;

– квантово-безпечні криптографічні протоколи, в першу чергу встановлення ключів;

– електронний підпис, захищений у постквантовий період.

За результатами даних досліджень прогнозується прийняття групи стандартів для постквантового періоду. Вже готові попередні версії кожного із проектів.

Орган зі стандартизації ЄС – ETSI опублікував груповий звіт «Квантово-захищена криптографія. Квантово-безпечна інфраструктура» [20], в якому закріплено основи перспективної інфраструктури, представлено механізми та наведені типи примітивів, що плануються використовувати. Окремо висунуто вимоги та сформовано критерії оцінки майбутніх кандидатів.

За результатами попередніх досліджень визначено п'ять сімейств криптографічних примітивів, в основу яких покладено математичні методи, що, на погляд спеціалістів, забезпечать виконання прогнозуємих вимог. У табл. 2 наведено дані відносно таких криптоперетворень та на чому базується їх стійкість.

Таблиця 2

Напрямки досліджень у постквантовій криптографії. Рекомендації ETSI

Lattice-based primitives	Криптографічна стійкість (безпека) залежить від складності розв'язання рівняння на алгебраїчних решітках
Multivariate primitives	Криптографічна стійкість (безпека) залежить від складності рішення системи багатовимірних поліноміальних рівнянь
Code-based primitives	Криптографічна стійкість (безпека) залежить від складності виконання завдання декодування лінійного коду
Hash-based primitives	Криптографічна стійкість (безпека) залежить від складності знаходження колізій або прообразів в криптографічних геш-функціях
Isogeny-based key primitives	Криптографічна стійкість (безпека) залежить від складності знаходження невідомої ізогенії між парою суперсінгулярних еліптичних кривих

У табл. 3 наведено дані відносно можливих криптографічних протоколів встановлення (узгодження, транспортування) ключів та відносно можливих механізмів автентифікації.

Таблиця 3

Класифікація постквантових примітивів встановлення ключів та механізмів ЕП

Примітиви узгодження ключів (key agreement primitives)	Дві сторони надійно генерують загальний симетричний ключ від інформації, що вноситься обома сторонами, наприклад шляхом захищеного обміну відкритими ключами один з одним, наприклад у вигляді сертифікатів відритих ключів.
Примітиви транспортування ключів (key transport primitives)	Одна з сторін генерує симетричний ключ і надійно розділяє його з іншою стороною, наприклад шляхом відправки його у зашифрованому вигляді відкритому ключі (сертифікату) іншої стороні
Схеми підпису типу Fiat-Shamir (Fiat-Shamir signature schemes)	Будуються на базі інтерактивних протоколів з доказо нульових знань
Схеми підпису на основі ґеш функцій (hash-and-sign signature schemes)	Будуються на основі використання односторонніх функцій

Також ETSI розроблено вимоги, які запропоновано висунути до кандидатів на постквантові стандарти криптографічних перетворень, що наведені у табл. 4. На їх основі в найближчий час планується оголосити Європейський конкурс на нові постквантові криптопримітиви з можливістю їх подальшої стандартизації.

Таблиця 4

Вимоги та параметри оцінювання кандидатів

Вимоги безпеки: - Проходження громадського контролю та визнання науковою спільнотою. - Надійне підтвердження криптографічної стійкості. - Актуальність моделі безпеки, якій відповідають криптопримітиви. - Стійкість криптопримітивів до існуючих, в тому числі на основі квантових алгоритмів, атак. - Можливість використання криптопримітивів в безпечних протоколах розподілу ключів. - Можливість поєднання кількох функцій безпеки криптографічних протоколів (наприклад, одночасна автентифікація та встановлення). - Можливість кількісної оцінки та порівняння заявлених класичних та квантових рівнів безпеки. - Визначеність рекомендованих розмірів ключів для заданих рівнів безпеки (наприклад, 80, 112 біт, 128 або 256 біт).	
Класична безпека	Стійкість проти класичних атак.
Квантова безпека	Стійкість проти «квантових» атак. Зокрема, стійкість до алгоритму Гровера.
Доказова безпека	Базування на задачах, які мають необхідну складність криптографічного аналізу. Можливе ігнорування зниження рівня складності за умови, що практична стійкість зміниться несуттєво.
Довгострокова безпека	Можливість використання у протоколах типу TLS 1.3 з підтримкою forward secure cipher suites.
Активна безпека	Стійкість проти атак з адаптивним підбором.
Ефективність	Використання рекомендованих параметрів розмірів загальних параметрів та ключів відповідно до заданого рівня безпеки. Незалежність швидкодії та кількості раундів перетворень від платформи реалізації. Допустима швидкодія генерації ключів і часу, необхідного для поширення нового ключа. Інші практичні вимоги (наприклад, стійкість до відмов).
Реалізація та розгортання	Простота впровадження стандартних примітивів нефахівцями. Відносно малий обсяг (ресурс) реалізації (зокрема, можливість реалізації на FPGA та вбудованих пристроях).

	Відносно малий (допустимий) обсяг необхідної пам'яті під час виконання (можливість реалізації на пристрої з обмеженими ресурсами). Практичність розмірів ключа і підпису для передачі або зберігання в ряді платформ, включаючи пристрої з обмеженими ресурсами. Простота інтеграції в існуючі криптографічні протоколи та криптографічні системи. Низька вартість заміни або модернізації захищених технологій. Можливість виконання криптопримітивів для декількох функцій, наприклад для забезпечення автентифікації, розподілу ключів тощо. Сумісність, наприклад гнучкість, у виборі ґеш-функції в схемах дерева Меркле тощо.

Важливим є той факт, що ENSI також висунув вимоги до розмірів параметрі та ключів ЕП. Відповідні дані наведені в табл. 5.

У табл. 5 надано результати порівняльного аналізу виконання основних операцій криптоперетворень [1]. У якості базової одиниці виміру береться час виконання відповідного перетворення на алгоритмі RSA.

Таблиця 5

Орієнтовні розміри параметрів та ключів для алгоритмів ЕП, що висунув NIST

Параметр Алгоритм	Час генерації ключів (RSA sign=1)	Час підпису (RSA sign=1)	Час перевірки (RSA sign=1)	Криптоперіод	Розмір відкритого ключа, біт	Розмір закритого ключа, біт	Розмір підпису (біт)
Winternitz-Merkle signatures	200 10000 500000	1 1 2	0.2 0.2 0.2	2^{20} 2^{30} 2^{40}	368 368 368	15200 22304 29344	17024 18624 20224
GLP signatures (lattice-based)	0.01	0.5	0.02		11800	1620	8950
CFS signature (code based)	5	2000	0.02		9437184	≈15000000	144
Psflash signature (multivariate)	50	1	0.1		576992	44400	296

Аналіз вимог до криптографічних примітивів постквантового періоду, що висунуті NIST США та ETSI ЄС, дозволяє зробити такі попередні висновки:

- вимоги NIST США та ETSI ЄС в основному дозволяють розпочати конкурс зі створення криптографічних примітивів, що будуть стійкими у постквантовий період;
- вимоги як NIST США так і ETSI ЄС не містять конкретних критеріїв оцінки та порівняльного аналізу потенційних кандидатів;
- нечіткими є визначення вимог до систем управління ключами, вони формулюються тільки відносно механізмів узгодження та транспортування ключів;
- в пропозиціях з оцінки стійкості (безпечності) використовується тільки довжина ключа симетричного криптографічного перетворення, допустимі значення довжин блоків відсутні, що, на наш погляд, не дозволяє отримати об’єктивних оцінок стійкості;
- допустимі довжини ключів у 128 бітів симетричних криптографічних перетворень є замалими, за рахунок цих особливостей можуть бути закладені вразливості;
- для оцінки стійкості та оцінки криптографічних примітивів при порівнянні та вибиранні кандидатів необхідно використовувати методики, що базуються на системах безумовних та умовних критеріїв, які дозволяють суттєво зменшити суб’єктивність прийняття рішень [3];

Висунуті NIST США та ETSI ЄС вимоги дозволяють, на наш погляд, зробити тільки попередні оцінки постквантових механізмів ЕП та приймати певні рішення відносно подальших їх досліджень з метою вибору найбільш ефективних за критеріями стійкості та техніко-економічними і техніко-експлуатаційними критеріями.

4. Порівняльний аналіз перспективних механізмів ЕП

В процесі попереднього аналізу та досліджень в якості постквантових механізмів були вибрані такі [1, 2, 24 – 33]:

- механізми ЕП на основі ґеш-функцій (HB-криптографія);
- механізми ЕП на основі збиткових кодів (CB-криптографія);
- механізми ЕП на основі перетворення на алгебраїчних решітках (LB-криптографія);
- механізми ЕП на основі мультиваріативного квадратичного перетворення (MQ-криптографія);
- механізми ЕП на основі ізогеній еліптичних кривих.

Розглянемо в узагальненому вигляді сутність названих вище кандидатів на стандарт постквантових механізмів ЕП та порівняємо їх, орієнтуючись на вимоги, що сформульовані в п. 2 та 3.

4.1. Сутність ЕП на основі ґеш-функцій (HB-кріптографія)

Механізми ЕП на основі ґеш-функцій грунтуються на використанні стандартної криптографічної ґеш-функції H, наприклад в [24 – 26] запропоновано формувати геш-значення з довжиною від 28 до b=128 бітів. Якщо для цього обрати ґеш-функцію SHA-256, то відкритий ключ підписувача в ній буде мати $8b^2$ бітів. Для вказаного значення b=128 відкритий ключ буде мати довжину у 16 кілобайт та складається з $4b$ строчок

$$Y_1[0],\ Y_1[1],\ Y_2[0],\ Y_2[1],\ \dots,\ Y_{2b}[0],\ Y_{2b},$$

кожна з яких має довжину $2b$ бітів. За цих умов, тобто для $b=128$, ЕП повідомлення m буде мати довжину $2b$ ($2b+1$) бітів, тобто 8 кілобайт. Підпис складається зі $2b$-бітових строчок $r, x_1,\dots, x_{2b}$, таких, що біти ($h_1,\dots, h_{2b}$) ґеш-значення $H(r, m)$ визначаються як

$$Y_1[h_1] = H(x_1),\ Y_2[h_2] = H(x_2)\ \dots\ Y_{2b}[h_{2b}] = H(x_{2b}).$$

З початку підписувач генерує секретний параметр x, а потім обчислює $Y=H(x)$.

Особистий ключ підписувача має $8b^2$ бітів, а саме – $4b$ незалежних однорідних випадкових строк $x_1[0], x_1[1], x_2[0], x_2[1], \dots, x_{2b}[0], x_{2b}[1]$, кожна з яких містить $2b$ бітів.

Після підписувач обчислює відкритий ключ

$$Y_1[0],\ Y_1[1],\ Y_2[0],\ Y_2[1],\ \dots,\ Y_{2b}[0],\ Y_{2b}[0]$$

у вигляді

$$H(x_1[0]),\ H(x_1[1]),\ H(x_2[0]),\ H(x_2[1]),\ \dots,\ H(x_{2b}[0]),\ H(x_{2b}[1])$$

При підписуванні повідомлення m підписувач генерує однорідну випадкову строчку T, обчислюючи біти ($h_1,\dots, h_{2b}$) ґеш-значення $H(r,m)$ та формує значення

$$(r,\ x_1[h_1],\ \dots,\ x_{2b}[h_{2b}]),$$

що і є електронним підписом повідомлення m. Далі підписувач знищує значення x, а значить більше не використовує його. Тобто це механізм, схожий на механізм одноразового *ЕП* Lomport-Diffie [25].

Якщо необхідно підписати більше, ніж одне повідомлення, то можна використовувати «зчеплення». В цьому випадку для підписання наступного повідомлення підписувач знову використовує згенерований відкритий ключ.

При верифікації перевірник перевіряє перше підписане повідомлення, а також включає до нього новий відкритий ключ. Після цього він зможе здійснити перевірку підпису наступного повідомлення. Підпис n-го повідомлення містить всі n-1 попередньо підписаних повідомлень.

Згідно з поглядами [1 – 7], криптографія на основі ґеш-функцій досить перспективний апарат, що може бути використаний у постквантових системах цифрового підпису. Криптографія на основі ґеш-функцій може використовувати будь-яку важко обернену функцію в

безпечну систему підпису на відкритих ключах. Це дозволить ефективно протистояти атаці, що грунтується на основі використання алгоритму Гровера [3, 6].

4.2. Механізми криптографічного перетворення з використанням збиткових кодів (СВ-криптографія)

Вважатимемо, що ціле b є ступенем двійки. Запишемо згідно [27 – 29] параметри збиткового коду

$$N = 4b \lg b;\ d = \lceil \lg n \rceil;\ t = 149$$

Відкритим ключем в такій системі є матриця K розмірністю $dt \times n$ з коефіцієнтами у полі F_2. Повідомлення представляє собою n-бітну строчку з вагою t, тобто n-бітна строка у своєму складі має точно t бітів, які дорівнюють 1. Для цього необхідно здійснити попереднє форматування повідомлення. Далі при зашифруванні повідомлення m відправник перемножує матрицю K на m та формує таким чином dt-бітний шифротекст

$$C = Km$$

Головною проблемою для зловмисника при криптоаналізі є пошук синдрому декодування матриці K. Тобто, для того щоб розв'язати цю систему рівнянь, необхідно знайти вхідний вектор з вагою t. Це можна зробити методами лінійної алгебри. Для цього необхідно виконати зворотню операцію відновлення Km для деякого n-бітного вектору ν, такого що $K\nu=Km$. Але для таких векторів існує експоненційно велика кількість векторів ν, тому пошук серед них t-вектора є також експоненційно складним. Найменш складною відомою атакою є атака зі складністю e^b для більшості матриць K.

При верифікації отримувач генерує відкритий ключ К з таємною структурою, а саме – з структурою прихованого коду Гоппа. Це дозволить отримувачу провести декодування у прийнятний час. Зрозуміло, що порушник може виявити структуру прихованого коду Гоппа у відкритому ключі, але на цей час така атака невідома.

Більш конкретно. Для випадку шифрування отримувач починає з особливих елементів $\lambda_1, \lambda_2, \ldots, \lambda_n$ у полі F_2d та таємного незвідного полінома системи t у полі $g \in F_2d\ [x]$. Основною складовою отримувача є формування синдрома декодування, тобто матрицю розмірністю $dt \times n$

$$H = \begin{pmatrix} 1/g(\lambda_1) & \cdots & 1/g(\lambda_n) \\ \vdots & \ddots & \vdots \\ \lambda_1^{t-1}/g(\lambda_1) & \cdots & \lambda_1^{t-1}/g(\lambda_n) \end{pmatrix}$$

В такій матриці кожен елемент є елементом поля F_{2^d} та розглядається як стовбчик із d елементів поля F_2 у стандартному базисі F_{2^d}. Ця матриця є частково контрольною матрицею для незвідного двійкового коду Гоппа і може бути декодована за допомогою алгоритму Патерсона або іншого швидкого алгоритму [27].

Відкритий ключ K є версією матриці H.

Таємний (особистий) ключ також містить інвертуєму матрицю S розмірністю $dt \times dt$ і матрицю перестановки P розмірністю $n \times n$. Відкритий ключ є результатом спеціального перетворення. Для того щоб отримати HPm, отримувач перемножує шифротекст $Km = SHPm$ на S , а потім декодує H, щоб отримати Pm. Наостанок він перемножує результат на матрицю P^{-1} та отримує відкритий текст m.

Особливості реалізації ЕП розглянемо на прикладі криптосистеми Нидерайтера. Вперше вона запропонована в [29] та отримала назву CFS ЕП. Доведення стійкості такої схеми зводиться до оцінки складності розвязку задачі синдромного декодування. Так, при відомому таємному ключі при декодуванні можна вирішити тільки для деякої долі випадкових слів. Для цього використовується багаторазове гешування повідомлення, яке рандомізоване засобом цього гешування з використанням лічильника з довжиною в r бітів. При цьому підписувач повинен використати свій ключ для визначення відповідного вектора помилки. Далі тає-

мний ключ використовується для визначення відповідного вектора помилок. Наостанок підписувач використовує цей вектор разом із значенням лічильника в якості підпису.

Розглянемо сутність та дамо оцінку стійкості такого механізму ЕП [29].

1. Генеруються загальні системні параметри: m, $t \in N$;

2. Генерується ключ генерації пари ключів як в системі Нідерайтера. Для цього використовується алгебраїчний код на основі ($n = 2m$, $k = n - mt$, $2t + 1$) двійкових незвідних поліномів Гоппи [28, 29]. Далі для нього породжуються такі матриці:

матриця H : $(n - k) \times n$, що є матрицею перевірки алгебраїчного коду, що має t виправляючу спроможність;

матриця X : $(n - k) \times (n - k)$ – випадкова обернена матриця;

матриця P : $n \times n$ – випадкова матриця перестановок.

Відкритим ключем є матриця $H_X = X \cdot H \cdot P$ та t виправляюча спроможність.

Таємним ключем є матриці X, P та швидкий алгоритм декодування алгебраїчного коду.

3. Обчислення підпису.

Вхідними даними є такі:

h – функція гешування, застосовується гешування вхідних даних x, результатом є геш-значення $h(x)$ з довжиною $n - k$ біт;

поліноміально-складний алгоритм декодування алгебраїчного коду, що застосовується до синдромної послідовності $s = (s_0, s_1, ..., s_{n-k-1})$;

відкритий текст M, для якого потрібно обчислити ЕП.

Вихідними даними є ЕП $У$ згідно механізму CFS для відкритого повідомлення M. Сутність алгоритму ЕП.

1. Обчислення геш-значення h(M) та присвоєння змінній і значення і =1.

2.Обчислення геш-значення h(h(M)) та його конкатенація.

3.Значення h(h(M)) розглядається як синдром у вигляді послідовності $s_X = (s_0, s_1, ..., s_{n-k-1})$, що обчислена для деякого довідного кодового слова та вектора помилок $e = (e_0, e_1, ..., e_{n-1})$.

4. Обчислюється значення вектору

$s_X^{*T} = X^{-1} \cdot s_X{}^T$,

та знаходиться вектор $\overline{e}^T = P \cdot e^T$.

5. Для послідовності (синдрому) $\overset{*}{S}_X$ здійснюється швидке декодування. Реалізується виконання швидкого алгоритму декодування та у разі успіху змінній присвоюється значення $i = i + 1$ та здійснюється перехід до 2.

6. Обчислюється значення вектору

$$e^T = P^{-1} \cdot \overline{e}^T = P^{-1} \cdot P \cdot e^T.$$

7. Обчислюється ЕП $Y = (e, i)$ для повідомлення М згідно зі схемою CFS.

8. Формиування ЕЦП за схемою CFS $Y = (e, i)$ для відкритого текста M.

Алгоритм перевірки (верифікації) здійснюється таким чином.

Вхідними даними є такі:

1. Відкритий ключ у вигляді матриці $H_X = X \cdot H \cdot P$ та число t.

2. Відповідна функція гешування h.

3. Швидкий з поліноміальною складністю алгоритм декодування.

4. Значення ЕП $Y = (e, i)$;

5. Відкритий текст M.

Алгоритм верифікації зводиться до виконання наступного.

1. Обчислення вектору здійснюється згідно механізмуCFS

$$s'_X = H_X \cdot e^T .$$

2. Обчислюється значення

$$s''_X = h(h(M)\|i);$$

3. Приймається рішення про правильність чи помилковість у вигляді: якщо $s'_X = s''_X$,то підпис правильний, інакше – помилковий.

Відносно стійкості механізму необхідно зазначити таке – згідно сучасних поглядів вона є експоненційно складною.

4.3. Сутність механізму на основі перетворення на алгебраїчних решітках (LB-криптографія)

Вперше сутність криптоперетворення на алгебраїчних решітках у 1996 р. запропонував M. Aitai [3, 12, 16, 17]. Решітка – це дискретна підмножина векторів (точок) у евклідовому просторі $\boldsymbol{R^n}$, яка є замкненою за операціями додавання та віднімання векторів. Решітка має розмірність *n*, якщо вона розміщується у будь-якому підпросторі простору $\boldsymbol{R^n}$. При геометричному поданні решітка – це множина, що рівноймовірно розміщена у просторі $\boldsymbol{R}$. За своїми властивостями алгебраїчна решітка є абелевою групою. Основою побудування алгебраїчної решітки *L* є множина векторів *B*, таких що будь-яка точка (вектор) *L* може бути представлений у вигляді лінійної комбінації елементів *B*. Стійкість LB-кріптосистем базується на складності вирішення двох комбінаторних проблем [16, 17]:

- найкоротшого вектору, вирішення якої зводиться до пошуку найкоротшого вектору у решітці *L* з базисом *B*;
- найближчих векторів, коли для заданого базису *B* решітки L и деякого вектору $\boldsymbol{v \in L}$ необхідно знайти вектор $\boldsymbol{v' \subset L}$, що є найближчим до вектору *v*.

Вказані проблеми у загальному випадку є експоненційно складними, наприклад для більшості базисів *B*. Якщо базисні вектори є короткими та ортогональними, то обидві проблеми можна ефективно вирішити. Пошук таких базисів на решітці називається редукцією базису решітки і для цього можна використати відомий алгоритм LLL [16, 17].

LB-криптосистеми можна поділити на дві такі групи:

- імовірно нестійкі, але ефективні криптосистеми, до яких можна віднести LB-криптосистеми, що грунтуються на перетвореннях в фактор-кільцях, наприклад NTRU-алгоритм [16, 17];
- імовірно стійкі, але не ефективні LB-криптосистеми. Як приклад такої криптосистеми можна назвати LWE-проблему (Learning with Errors). Складність такої криптосистеми (Ring-LWE) грунтується на комбінаторній проблемі, яка дозволяє будувати криптосистеми, що є відносно ефективні і стійкі до атак із застосуванням квантових комп'ютерів. Механізми побудування таких криптосистем та оцінки їх властивостей (попередні) можна знайти в [16, 17].

4.4. Сутність механізму ЕП на основі мультиваріативного квадратичного перетворення (MQ-криптографія)

Розглянемо сутність механізму ЕП на основі мультиваріативного квадратичного перетворення, спираючись на [1, 2, 30, 31].

Відкритий ключ в мультиваріативній криптосистемі є послідовністю P1, P2,…, P2b ∈ F2 [ω1, …, ω4b]

Із 2b поліномів з 4b змінних. ω1, …, ω4b з коефіцієнтами у полі F2 ∈ {0,1}. Кожний поліном має мати що найбільш ступень 2, без квадратичних термів, та представлений як послідовність 1, ω1, …, ω4b, ω1ω2, ω1ω3, …, ω4b-1ω4b.

В цілому, відкритий ключ має 16b3+4b2+2b бітів. Наприклад, для b = 128, об'єм ключа складатиме 4 Mbyte.

Суттєвою перевагою ЕП на основі MQ-криптографії, наприклад над НВ-підписом, є те, що підпис є коротким. Інші MQ-системи мають ще коротші підписи і у ряді випадків більш короткий відкритий ключ.

Основною проблемою для криптоаналітика відносно MQ-криптографії є пошук послідовності з 4b ω1, …, ω4b бітів, що породжує 2b вище зазначених вихідних бітів

(P1(ω1, …, ω4b), …, P2b(ω1, …, ω4b)).

Ймовірність вгадування послідовності з 4b бітів можна оцінити як 2^{-2b}.

ЕП виконується таким чином.

Зафіксуємо стандартний незвідний поліном $\varphi \in F_2(t)$ ступеня 3b. Визначимо L як поле $F2(t)/_{\varphi}$ розмірністю 2^{3b}. Критичним кроком під час формування підпису є пошук кореня таємного одномірного (uniraviate) поліному малого ступеня над L, а саме, полінома в $L[x]$ зі ступенем не більше ніж $2b$. Існує декілька стандартних алгоритмів для вирішення цієї задачі за час $b^{O(1)}$.

Таємний поліном обирається таким чином, щоб мати всі ненульові експоненти виду 2^i+2^j або 2^i.

Якщо елементи $x \in L$ представлені у вигляді

$$x_0+x_1t_1+\ldots+x_{3b-1}, \text{ де } x_i \in F_2,$$

тоді

$$x_2=x_0+x_1t^2+\ldots+x_{3b-1}t^{6b-2}$$
$$x_4= x_0+x_1t^4+\ldots+x_{3b-1}t^{12b-4.}$$

і т.і.

Таким чином, $x^{2i}+^{2j}$ є квадратичним поліномом із змінними $x_0, \ldots, x_{3b-1}$.

Деякі прості перетворення приховують структуру цього полінома і породжують відкритий ключ.

Таємний ключ підписувача має три компоненти:

1.Оборотну матрицю S розмірністю $4b \times 4b$ з коефіцієнтами в F_2

2. Поліном $Q \in L\ [x, \nu_1, \nu_2, \ldots, \nu_b]$, де кожний терм має одну з шести можливих форм:

$$l\, x^{2^i+2^j},$$
де $l \in L$, $2^i < 2^j$, $2^i + 2^j \leq 2b$;
$$\text{де } l\, x^{2^i} \nu_j,$$
де $l \in L$, $2^i \leq 2b$;
$$l\nu_1\, \nu_j$$
$$l\, x^{2^i}$$
$$l\nu_j$$
$$l$$

Якщо b=128, то маємо 944b можливих термів, кожний з яких має 384-бітний коефіцієнт l, а загальний об'єм 443 Кбіт.

3. Матрицю T розмірністю $2b \times 3b$ рангу $2b$ з коефіцієнтами у F_2.

Підписувач обчислює відкритий ключ таким чином:

$(x_0, x_1, \ldots, x_{3b-1}, \nu_1, \nu_2, \ldots, \nu_b)$ як S раз вектору $(\omega_1, \ldots, \omega_{4b})$ всередині фактор-кільця $L[\omega_1, \ldots, \omega_{4b}]/(\omega_1^2 - \omega_1, \ldots, \omega_{1b}^2 - \omega_{4b})$.

Обчислює

$$x = \sum x_i t^i \text{ та}$$
$$y = Q(x, \nu_1, \nu_2, \ldots, \nu_b).$$

Подає y у вигляді

$$Y_0 + Y_1 t + \cdots + Y_{3b-1} t^{3b-1}$$

де кожний $Y_i \in F_2\ [\omega_1, \ldots, \omega_{4b}]$, та обчислює $(P_1, P_2, \ldots, P_{2b})$.

Підписування є зворотним. Воно здійснюється таким чином.

1.Починаючи з величини $P_1, P_2, \ldots, P_{2b}$, вирішуємо таємне лінійне рівняння $T(Y_0, Y_1, \ldots, YP_{3b-1}) = (P_1, P_2, \ldots, P_{2b})$ для того, щоб отримати значення $(Y_0, Y_1, \ldots, Y_{3b-1})$. Існує 2^b можливих варіантів рішення для $(Y_0, Y_1, \ldots, Y_{3k-1})$. Обираємо випадковим чином одне із них.

2. Обирається випадково значення $v_1, v_2, \ldots, v_b, \in F_2$ і підставляємо його у таємний поліном $Q(x, v_1, v_2, \ldots, v_b)$, отримуючи поліном $Q(x) \in L[x]$

3.Обчислюється $Y = Y_0 + Y_1 t + \cdots + Y_{3b-1} t^{3b-1} \in L$ та вирішується $Q(x) = Y$, отримуємо $x \in L$. Якщо існує декілька коренів, починаємо процес з початку.

4.Записується x як

$$x_0 + x_1 t + \cdots + x_{3b-1} t^{3b-1}$$

де $x_0, x_1, x_{3b-1} \in F_2$.

Вирішується таємне рівняння

$$S(\omega_1, \ldots, \omega_{4b} = (x_0, \ldots, x_{3b-1}, v_1, \ldots, v_b)$$

та отримується підпис.

Далі, *HFE*-приховане рівняння в полі $Q(x) = Y$ з пропуском декількох бітів.

Тобто $Q(x) = Y$ є еквівалентом 3*b* рівнянь, але публікується тільки 2*b* рівнянь, де «v» – означає «vinegar», змінні $v_1, v_2, \ldots, v_b$.

Необхідно відмітити, що HFE перетворення, тобто без пропусків бітів та без *v*-змінної може бути атаковано за $2^{(lgb)^2}$ операцій при застосуванні атаки Grobner але HFE^v-перетворення буде протистояти такій атаці.

4.5. Сутність механізму на основі ізогеній енліптичних кривих

Ізогенія – це раціональне відображення $\varphi: E_1(K) \to E_2(K)$, де $E_1(K)$ та $E_2(K)$є еліптичними кривими, а $\varphi(P_\infty) = P_\infty$[32 – 33]. Нульова ізогенія – це ізогенія, що відображає усі точки однієї кривої, у точку на нескінченності іншої. Ядром ізогенії є $Ker\ (\varphi) = \{K_i \in E_1\};\ \varphi\ (K_i) = P_\infty$.

Ізогенії ініціюють відображення полів функцій на кривих. Степінь розширення $(K(E_1): \varphi * K(E_2))$ називається степінню ізогенії.

Для ізогенії $\varphi: E_1(K) \to E_2(K)$ існує дуальна ізогенія $\hat{\varphi}: E_2(K) \to E_1(K)$, така, що $\hat{\varphi}\varphi = [l]$, де l – множення точки кривої E_1 на число l, аналогічно $\varphi\hat{\varphi} = [l]$, де l – множення точки кривої E_2 на число l. Дуальні ізогенії мають однакову степінь.

У випадку алгебраїчно замкненого поля операція множення точки на число l задає ендоморфізм еліптичної кривої з ядром l^2 точок. Оскільки ізогенія відповідає квадратному кореню з операції множення на l, то ядро ізогенії складається з l точок порядку l, що створюють циклічну групу (однією з них є точка P_∞).

Ізогенії складних степенів можуть використовуватися як композиція ізогеній простих степеней.

Властивості ізогеній, що використовуються при створенні криптосистем:

1) $\gamma\ (\varphi\ (A)) = \varphi\ (\gamma\ (A)) = \gamma\varphi(A)$;

2) $k * A_\varphi = \varphi\ (k * A)$.

Знаходження ізогеній по ядру. Для знаходження ізогенії $\varphi: E_1(K) \to E_2(K)$ з заданим ядром використовується формула Велу [32, 33].

Для еліптичної кривої, що задана формулою Вейєрштрасса:

$$E_1 : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Нехай *C* – группа точок еліптичної кривої, що буде ядром ізогенії. Тоді:

1. Формуємо набір точок *S*:

а) Виключаємо з С точку на нескінченності.

б) Нехай C_2 – усі точки *C*, в яких координата *y* дорівнює нулю, а *R* – усі інші точки *C*.

в) Розділимо точки набору *R* на R_+ та R_- таким чином, що для кожної точки *P*, що належить R_+ , *-P* належить R_-.

г) $S = R_+ \cup C_2$.

2.Для кожної точки $Q \in S$ виконуємо наступні обчислення:

а) $g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q$;

б) $g_Q^y = -2y_Q - a_1x_Q - a_3$;

в) $v_Q = \begin{cases} g_Q^x, & 2Q = \infty \\ 2g_Q^x - a_1g_Q^y, & 2Q \neq \infty \end{cases}$;

г) $u_Q = (g_Q^y)^2$;

ґ) $v = \sum_{Q \in S} v_Q$;

д) $w = \sum_{Q \in S} (u_Q + x_Q v_Q)$.

3. Розраховуємо формулу еліптичної кривої $E_2(K)$:

а) $A_1 = a_1$;

б) $A_2 = a_2$;

в) $A_3 = a_3$;

г) $A_4 = a_4 - 5v$;

ґ) $A_6 = a_6 - (a_1^2 + 4a_2)v - 7w$;

д) $E_2: y^2 + A_1xy + A_3y = x^2 + A_2x^2 + A_4x + A_6$.

4. Розраховуємо координати точки $(x_\varphi, y_\varphi) = \varphi(x,y)$:

а) $x_\varphi = x + \sum_{Q \in S}\left(\frac{v_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2}\right)$;

б) $y_\varphi = y - \sum_{Q \in S}\left(u_Q\frac{2y + a_1x + a_3}{(x - x_Q)^3} + v_Q\frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - g_Q^xg_Q^y}{(x - x_Q)^2}\right)$

Отримані формули на кроці 4 будуть ізогенією з заданим ядром.

Оскільки в криптографії еліптичних кривих прийнято використовувати спрощену формулу Вейєрштрасса, то ми приведемо до прийнятого вигляду:

$$E_1: y^2 - x^3 + a_4x + a_6$$

Нехай *C* – группа точок еліптичної кривої, що буде ядром ізогенії. Тоді:

1. Формуємо набір точок *S*:

а) Виключаємо з С точку на нескінченності.

б) Нехай C_2 – усі точки *C*, в яких координата *y* дорівнює нулю, а *R* – усі інші точки *C*.

в) Розділимо точки набору *R* на R_+ та R_- таким чином, що для кожної точки *P*, що належить R_+ , *-P* належить R_-.

г) $S = R_+ \cup C_2$.

2. Для кожної точки $Q \in S$ виконуємо наступні обчислення:

а) $g_Q^x = 3x_Q^2 + a_4$;

б) $g_Q^y = -2y_Q$;

в) $v_Q = \begin{cases} g_Q^x, & 2Q = \omega \\ 2g_Q^x, & 2Q \neq \infty \end{cases}$;

г) $u_Q = (g_Q^y)^2$;

ґ) $v = \sum_{Q \in S} v_Q$;

д) $w = \sum_{Q \in S} (u_Q + x_Q v_Q)$.

3. Розраховуємо формулу еліптичної кривої $E_2(K)$:

а) $A_4 - a_4 - 5v$;

б) $A_6 = a_6 - 7w$;

в) E_2: $y^2 = x^2 + A_4x + A_6$.

4. Розраховуємо координати точки $(x_\varphi, y_\varphi) = \varphi(x,y)$:

а) $x_\varphi = x + \sum_{Q \in S}\left(\frac{v_Q}{x-x_Q} + \frac{u_Q}{(x-x_Q)^2}\right)$;

б) $y_\varphi = y - \sum_{Q \in S}\left(u_Q \frac{2y}{(x-x_Q)^3} + v_Q \frac{y-y_Q}{(x-x_Q)^2} - \frac{g_Q^x g_Q^y}{(x-x_Q)^2}\right)$.

5. Порівняльний аналіз ЕП для постквантового періоду

В цьому розділі наводяться попередні результати порівняльного аналізу криптографічних перетворень, що є кандидатами постквантового періоду..

У табл. 6 надаються загальні характеристики математичного апарату, на яких грунтуються механізми ЕП, з використанням яких можуть бути розроблені квантово-захищені алгоритми ЕП. Скоріше всього перспективними є методи HB та MQE-криптографії, у той час як механізми направленого (асиметричного) шифрування скоріше всього на основі LB та CB-криптографії.

Наведені в табл. 7 механізми ЕП були запропоновані робочою групою ETSI для подальшого вивчення і дослідження у якості можливих кандидатів на квантово-захищені схеми ЕП.

Таблиця 6

Характеристики напрямків, у яких можуть бути розроблені квантово-захищені алгоритми

Криптографічна схема	Підпис	Шифрування	Розмір ключа	Тип даних	Core Ops.	Cryptographic Maturity
Hash-Based	Yes	No	≈20	Hash outputs	Hashing	High
Multivariate Quadratic	Yes	No	≈10k	$GF(2^m)$	Matrix mult. LSE solving	Low, medium for conservative schemes
Lattice-Based: NTRU General lattice	 Maybe Maybe	 Yes Yes	 <0.1k ≈100k	 Z_q $GF(2^m)$	 Convolution Matrix mult.	 Medium Medium
Code-Based	Expensive	Yes	≈100k	$GF(2^m)$	Matrix mult. decoding	High, with precautions to implementation

Таблиця 7

Порівняння довжин ключів та підписів для квантово-захищених алгоритмів

Тип	Схема	Безпечність (бити)	Відкритий ключ (байти)	Підпис (байти)
Lattice	Lyubashevsky	-------	1 664	2 560
	NTRU-MLS	128	988	988
	Aguilar et al	128	1 082	1 894
	Guneysu te al	80	1 472	1 120
	BLISS	128	896	640
	Ducas et al	80	320	320
	HIMMO	128	32	-----

MQ	Quartz	80	72 237	16
	Ding	123	142 576	21
	UOV	128	413 145	135
	Cyclic-UOV	128	60 840	135
	Rainbow	128	139 363	79
	Cyclic-Rainbow	128	48 411	79
Code	Parallel-CFS	120	503 316 480	108
	Cayrel et al	128	10 920	47 248
	Cyclic-Cayrel et al	128	208	47 248
	RankSign	130	7 200	1 080
	Cyclic-RankSign	130	3 538	1 080
Hash	Merkle	128	32	1 731
	Leighton-Micali	128	20	668
	XMSS	256	64	8 392
	SPHINCS	256	1 056	41 000
Isogeny	Jao-Soukharev	128	768	1 280
	Sun-Tian-Wang	128	768	16

Таким чином, на цей час досі ще важко визначити конкретну схему постквантового ЕП. Кожний з представлених варіантів має свої переваги та недоліки. У перспективі доцільно провести дослідження та уведення більш обґрунтованої методики та критеріїв порівняння ЕП постквантового періоду. На наш погляд, для порівняльного аналізу може бути використана методика, що грунтується на застосуванні системи безумовних та умовних критеріїв та обчисленні на їх основі безумовного та умовного інтегральних критеріїв.

Висновки

1. При побудові моделей загроз у постквантовий період в якості основних необхідно брати методи криптоаналізу як основні моделі загроз, що можуть бути реалізованими на квантовому комп’ютері при вирішенні задач криптоаналізу. Вказані методи повинні бути орієнтовані на використання специфіки квантового комп’ютера та мову програмування на ньому.

2. До основних задач, які можуть бути вирішені на квантовому комп’ютері, при реалізації загроз в першу чергу необхідно віднести такі:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в скінченному полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор-кільці.

3. У 2015 р. фахівці компанії Google підтвердили, що згідно з їх дослідженням в комп'ютері D-Wave використовуються квантові ефекти. Причому в «1000-кубітному» комп'ютері кубіти в дійсності організовані в кластери по 8 кубіт кожен. Це дозволило добитися в одному з алгоритмів швидкодії в 100 млн разів більше ніж у звичайному комп'ютері.

4. До можливих кандидатів на ЕП сформульовані такі мінімальні вимоги:

- відкритість алгоритму ЕП для криптографічної спільноти та їх аналізу;
- можливість реалізації ЕП у широкому діапазоні існуючих платформ;
- забезпечення, як мінімум, функції ЕП та її застосування у криптографічних протоколах, а також для направленого шифрування;
- наявність теоретичних та емпіричних доказів щодо забезпечення вимог безпеки (стійкості).

Більш конкретні вимоги формулюються у трьох напрямках: вимоги з безпеки (вимоги до стійкості до криптографічного аналізу), техніко-економічні вимоги (обчислювальні витрати та витрати на пам’ять) та технічні характеристики реалізації алгоритмів. У [1] наведено вимоги NIST до постквантових криптографічних примітивів. Наведені дані містять вимоги та

рекомендації що першого етапу розроблення та тестування постквантових примітивів. Вони охоплюють широкий спектр та містять вимоги до безпеки постквантових криптографічних примітивів, техніко-економічні та техніко-експлуатаційні вимоги. Також запропоновано узагальнені критерії оцінки та порівняння можливих кандидатів.

5. На сьогодні ще остаються відкритими питання встановлення конкретних значень вказаних показників та визначення критерів порівння. Протягом 2016 р. ці параметри будуть визначені групою експертів. Сьогодні NIST також надає деякі орієнтовні значення для окремих параметрів.

6. Наведені в табл. 1 та 4 результати дозволяють зробити попередні оцінки постквантових механізмів ЕП та приймати рішення відносно подальших їх досліджень з метою вибору для стандартизації більш перспективних. У табл. 4 наведені дані відносно таких криптоперетворень та на чому базується їх стійкість.

7. В процесі попереднього аналізу та досліджень в якості постквантових механізмів були вибрані такі механізми ЕП:

на основі ґеш-функцій (HB-критографія);
збиткових кодів (CB-криптографія);
основі перетворення на алгебраїчних решітках (LB-криптографія);
основі мультиваріативного квадратичного перетворення (MQ-криптографія);
основі ізогеній еліптичних кривих.

8. У табл. 2 та 4 наведено загальні характеристики математичного апарату, на яких грунтуються механізми ЕП, з використанням яких можуть бути розроблені квантово-захищені алгоритми ЕП. На наш погляд, перспективними є методи HB та MQE-криптографії, у той час як механізми направленого (асиметричного) шифрування скоріше всього будуть побудовані на основі LB та CB-криптографії.

Список літератури: 1. *A RIDDLE* WRAPPED IN AN ENIGMA. NEAL KOBLITZ AND ALFRED J. MENEZES Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A 2. *Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone.* Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT). https://www.google.com.ua/search? 3. *Горбенко, Ю.І.* Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія ; зааг. ред. І.Д. Горбенко. – Харків : Форт, 2015. – 959 с. 4. *Горбенко, Ю. І.* Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю.І. Горбенко, Р.С. Ганзя. // Східно-європейський журнал передових технологій. – 2014. – № 1/9 (67). – С. 8–15. 5. *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. 6. *Grover, L. K.* A fast quantum mechanics algorithm for database search / L. K. Grover // – Proceeding of the 7. *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 8. *Lenstra, H. W.* Analysis and Comparison of Some Integer Factoring Algorithms, in Computational Methods in Number Theory / H. W. Lenstra, Jr. and R. Tijdeman, eds. // Math. Centre Tract 154 – 1946 – P. 89. 9. *Горбенко, Ю. І.* Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем / Ю. І. Горбенко, Р. С. Ганзя // Східно-європейський журнал передових технологій. – 2014. – № 1/9 (67). – С. 8–15. 10. *Горбенко, Ю. І.* Аналіз стійкості популярних криптоситем протиквантового криптоаналізу на основі алгоритму Гровера / Ю. І. Горбенко, Р. С. Ганзя // інформації. – 2014. – Т. 16, №2. – С. 22–28. 11. *Ганзя, Р. С.* Квантовий криптоаналіз перетворень в групі точок еліптичних кривих / Р.С. Ганзя, Ю.І. Горбенко // Спеціальні телекомунікаційні системи Захист та захист інформаціцї. Збірник наук. праць. – 2012. – Вип. 2(22). – С 17-30. 12. *Ганзя, Р. С.* Методи здійснення атак на NTRU на основці квантових алгоритмів та їх порівняльний / Р.С. Ганзя, Ю.І. Горбенко // Спеціальні телекомунікаційні системи та захист інформаціцї. Зб. наук. праць. – 2013. – Вип. 2(23). – С. 9 – 17. 13. *Горбенко, Ю. І.* Аналіз стійкості постквантових систем / Ю. І. Горбенко. Р. С. Ганзя // Прикладная радиоэлектроника. – 2014. – Т. 13. – № 3. – С. 268–274. 14. *Горбенко, Ю. І.* Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю. І. Горбенко, Р. С. Ганзя // Комп'ютерні системи та мережі : Вісник національного університету «Львівська політехніка». – 2014. – № 806. – С. 40–49. 15.*Wang, X.* A quantum algorithm

for searching a target solution of fixed weight / Wang, X. W. . S. Bao and X. Q. Fu// Chinese Sci Bull. – 2002. – Vol. 55(29). – P. 484–488. 16. *Wang, H.* An efficient quantum meet-in-the-middle attack against NTRU-2005 / Wang Hong, MA Zhi, MA ChuanGui // Chinese Science Bulletin. – 2013. – Vol. 58, No. 28–29. – P. 3514–3518. 17. *X. Wang, W. S. Bao and X. Q. Fu.* A quantum algorithm for searching a target solution of fixed weight. – 2010. – Chinese Sci Bull, 55(29). 18. *Deputy* Chief Designer JSC Institute of Information Technology www.iit.com.ua 19.*Quantum* Safe Cryptography and Security. An introduction, benefits, enablers and challenges. ETSI White Paper No. 8 – 2015. 20. *ETSI GR* QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 21. *Moody D*. Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography, Japan, 2016. Режим доступу: [https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf] 22. D-Wave Systems: official site (англ.). 23.Quantum entanglement. The requested URL /content/view/40/60/ was not found on this server. 24. *McGrew D., Curcio M*. Hash-Based Signatures draft-mcgrew-hash-sigs-00[Электронный ресурс] / D. McGrew, M. Curcio – Режим доступа: https://tools.ietf.org/html/draft-mcgrew-hash-sigs-00. 25. *McGrew D., Curcio M.* Hash-Based Signatures draft-mcgrew-hash-sigs-01[Электронный ресурс] / D. McGrew, M. Curcio – Режим доступа: https://tools.ietf.org/html/draft-mcgrew-hash-sigs-01. 26.*ETSI* GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 27. *ETSI* White Paper №8: Quntum safe cryptography and security. – 2015. 28. *NIST* PQC workshop: SAFEcrypto Project, M. O'Niell. – 2015. 29. *Інтернет-ресурс* http://www.nkj.ru/archive /articles/5309/. 30. *Feyman, R.P.* Quantum mechanical computers // Opt. News, February. – 1985. №11. – P.p. 11-39. 31. *Reinier Broker*. Constructing supersingular elliptic curves // Comb. Number Theory, (3): pp. 269–273, 2009. 32. *Steven D. Galbraith*. Constructing isogenies between elliptic curves over Finite Fields. LMS J. Comput. Math,. 2: pp. 118–138 (electronic), 1999. 33. *David Jao and Luca De Feo.* Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies // Bo-Yin Yang, editor, PQCrypto, volume 7071 of Lecture Notes in Computer Science, pp. 19–34. Springer, 2011.

Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 04.09.2016