ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.01**

І.Д. ГОРБЕНКО, д-р техн. наук, А.М. ОЛЕКСІЙЧУК, д-р техн. наук,
О.Г. КАЧКО, канд. техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук,
М.В. ЄСІНА, канд. техн. наук, С.О. КАНДІЙ

МЕТОДИ ОБЧИСЛЕННЯ СИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ ЕЛЕКТРОННОГО ПІДПИСУ «CRYSTALS-DILITHIUM» 128, 256, 384 ТА 512 БІТ РІВНІВ БЕЗПЕКИ

Вступ

Наразі спостерігається стійкий прогрес у створенні квантових комп'ютерів різних призначень та можливостей, одним із основних призначень є здійснення криптоаналізу існуючих асиметричних криптосистем [1, 3]. Практично завершується створення математичних основ та програмного забезпечення для таких квантових комп'ютерів [4 – 11]. Особлива увага приділяється розробці великомасштабних квантових комп'ютерів, що призначаються для криптоаналізу існуючих стандартизованих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення [9, 11]. Залишаються певні сумніви щодо симетричних криптоперетворень типу гешування, блокового та потокового симетричного шифрування. Але, як показують дослідження, збільшення при їх використанні розмірів параметрів та ключів згідно з нинішніми поглядами дозволяє забезпечити криптографічний захист на далеку перспективу. Зважаючи на можливості зламу існуючих асиметричних криптосистем, Національний інститут стандартів і технологій (NIST) США прийняв рішення у вигляді проєкту стандарту NIST 8309 щодо другого раунду конкурсу на перспективні стандартні алгоритми електронного (цифрового) підпису (ЕП) [2, 3].

Прийняті нові стандартизовані алгоритми ЕП дозволять реалізувати системи ЕП, що будуть здатні захистити конфіденційну інформацію уряду США в доступному для огляду майбутньому, в тому числі після появи квантових комп'ютерів. Таким чином, однією з основних проблем сучасної криптографії на міжнародному рівні є створення стандартизованих криптографічних систем (схем), які були б безпечними у постквантовий період. Таким чином, на світовому рівні зусилля значного числа криптологів, математиків та криптологів-практиків зосереджені на відкритому конкурсі NIST PQC [1 – 4, 12 – 18], одним із основних завдань якого є розробка та прийняття постквантового чи постквантових стандартів ЕП. Його підсумком є визначення фіналістів другого етапу конкурсу у вигляді проєктів CRYSTALS-DILITHIUM, FALCON та Rainbow [2, 3]. Окрім цього, були визначені три альтернативних кандидати, які потребують більш детальних досліджень уже на четвертому етапі конкурсу – GeMSS, Picnic та SPHINCS+[2].

Аналіз показує, що в Україні є розуміння існування загроз стандартизованим існуючим асиметричним криптоперетворенням. Так, розроблено та прийнято національний стандарт «Алгоритми асиметричного шифрування та інкапсуляції ключів» [2, 3], що побудований на основі застосування алгебраїчних решіток. Особливістю цього стандарту (ДСТУ 8961-2019) [12] є суттєве підвищення криптографічної стійкості асиметричного шифрування та інкапсуляції ключів у перехідний та постквантовий період. На відміну від пропозицій та можливостей, що затверджені та прийняті NIST 8309 [2], є можливість використовувати його з рівнями безпеки 384 та 512 бітів. Найвищий рівень безпеки проєктів CRYSTALS-DILITHIUM, FALCON та Rainbow 256 бітів проти класичного та 128 бітів квантового криптоаналізу.

В той же час наші дослідження показали, що з урахування можливостей щодо забезпечення безпеки з використанням уже прийнятих в Україні симетричних криптоперетворень ДСТУ 7564-2014, ДСТУ 7624-2014 та ДСТУ 8845-2019 [12], національні стандарти ЕП повинні забезпечити в перспективі до 512 біт класичної та 256 біт квантової безпеки.

Аналіз показав [2, 17, 18], що серед схем ЕП на решітках суттєві переваги надано проєктам ЕП CRYSTALS – DILITHIUM та FALCON, вони рекомендовані для подальшого дослідження та стандартизації в процесі третього етапу конкурсу. Причому кращими визначено як математичні основи, так і алгоритми ЕП CRYSTALS – DILITHIUM [3, 16 – 18]. ЕП CRYSTALS-DILITHIUM досліджувався у другому раунді як один із трьох проєктів ЕП на основі решітки. Його безпека грунтується на складності MLWE задачі криптоаналізу та задачі модульного короткого цілого рішення (MSIS) [17, 18]. Основою побудови алгоритму ЕП CRYSTALS–DILITHIUM є використання алгоритму Fiat-Shamir [17] з перериваннями. В ньому використовуються один і той же модуль і кільце поліномів для всіх наборів параметрів, а ентропія забезпечується за допомогою рівномірного розподілу. Це призводить, у порівнянні з гаусовим розподілом проєкту ЕП FALCON, до більш простої реалізації.

Загалом DILITHIUM має високі, збалансовані показники щодо розміру ключів та підписів, а також щодо ефективності алгоритмів генерації ключів, підпису та перевірки. DILITHIUM добре працює в реальних експериментах. Також у другому раунді до реалізації DILITHIUM додано опцію випадкової генерації підпису, що заснована на використанні AES. Це дало майбутні переваги при апаратних реалізаціях інструкцій ЕП. Крім того, було опубліковано нове дослідження безпеки в QROM [45], яке стосується DILITHIUM.

NIST рекомендував розробникам ЕП DILITHIUM додати набір параметрів 5-го рівня безпеки (5-й – за нашою класифікацією це 1-й рівень безпеки із 4-х рівнів). Також необхідні додаткові дослідження розуміння конкретної безпеки, оскільки DILITHIUM має найнижчий набір параметрів безпеки CoreSVP [2, 3] з усіх схем на основі решітки, які все ще знаходяться в процесі досліджень та порівняння. В той же час NIST вибрав DILITHIUM як фіналіста і очікує, що або DILITHIUM, або FALCON будуть стандартизовані як основна схема постквантового підпису в кінці третього раунду.

Необхідно відмітити, що в процесі формування вимог до ЕП NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на нашу думку, на перспективу доцільним є використання в DILITHIUM, 384 і 512 біт безпеки проти класичного криптоаналізу та 192 та 256 біт безпеки проти квантового криптоаналізу. Але, як показали дослідження, як з точки зору теорії так і практики, генерація загальносистемних параметрів для використання 256, 384 і 512 біт безпеки проти класичного криптоаналізу та 128, 192 та 256 біт безпеки проти квантового криптоаналізу, які в фіналісті CRYSTALS-DILITHIUM не реалізовано. Будемо також вважати, що відносно побудування ЕП CRYSTALS-DILITHIUM для 128 класично та 64 біт квантової стійкості проблем немає [3, 16].

Під час ухвалення рішення стосовно фіналістів на прийняття стандарту ЕП в третьому раунді кращими та отримали рекомендації визначені проєкти ЕП CRYSTALS-DILITHIUM та FALCON. В оцінці NIST ці проєкти на основі структурованої решітки представляються найбільш перспективними та універсальними алгоритмами для електронного підпису, асиметричного шифрування та протоколу інкапсуляціє ключів [2, 12 – 18].

Метою статті є обгрунтування моделі безпеки, класифікація, первинний аналіз та оцінка відомих атак на криптосистему ЕП CRYSTALS–DILITHIUM, встановлення обмежень та розробка практичних алгоритмів обчислення (генерації) загальносистемних параметрів для за-

безпечення 128, 256, 384 і 512 біт безпеки проти класичного та 64, 128, 192 та 256 біт проти квантового криптоаналізу.

1. Сутність криптографічних перетворень фіналіста ЕП конкурсу NIST США «CRYSTALS-DILITHIUM»

У [2, 3, 16] наведено пропозиції та результати досліджень щодо сутності, властивостей та умов застосування кандидата на постквантовий стандарт ЕП Crystals-Dilithium (в подальшому Dilithium), що були сформовані та подані на конкурс NIST. На першому етапі досліджень в 2018 р. виявлені певні проблемні питання, щодо яких авторами проєкту стандарту були обґрунтовані та запропоновані певні удосконалення механізму ЕП Dilithium [3]. У цьому розділі розглянемо сутність та основні математичні та криптографічні положення Dilithium, що будуть потрібні для оцінки криптографічної стійкості. Причому, особливу увагу звернемо на рівні криптографічної стійкості, тобто 1 – 5 рівні стійкості [1, 2], що рекомендуються та можуть бути реалізованими поки ще в проєкті стандарту ЕП Dilithium. Відмітимо, що одним із основних проблемних питань, будемо мати на увазі обґрунтування необхідності та розробки удосконаленої версії ЕП Dilithium, що може забезпечувати в постквантовий період 128, 256, 384 і 512 біт безпеки проти класичного та 64, 128, 192 та 256 біт проти квантового криптоаналізу від найбільш загрозливих атак [2, 16 – 18].

Метод (схема) ЕП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями" [3, 17]. Він в певній мірі схожий на схему, що запропонована з послідовним удосконаленням в [16, 17]. Для спрощеного та узагальненого подання механізму розглянемо спрощену його версію на рис. 1 [3, 16], на якому наведено алгоритми генерації ключа, вироблення та перевірки ЕП. Основні положення та вирішення задачі обчислення (генерування) системних параметрів удосконаленого ЕП Dilithium наведені у параграфі 4 статі.

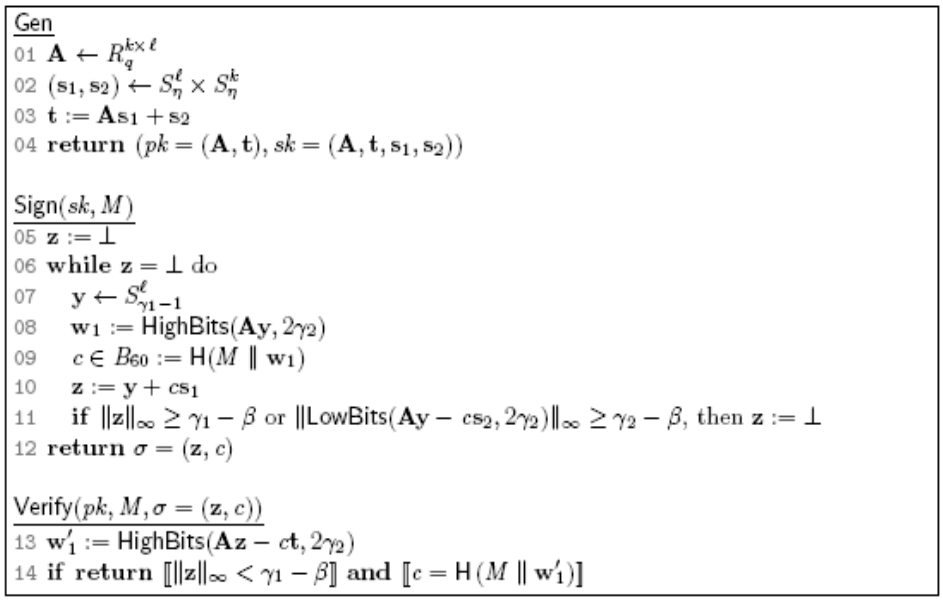


Рис. 1. Шаблон для механізму ЕП без стиснення відкритого ключа

1.1. Генерація основних складових ключа

Спочатку (рядок 01, рис. 1) генерується матриця поліномів **A** розміру $k \times \ell$, кожен з елементів якої є поліномом у кільці $R_q = \square_q[X]/(X^n + 1)$. В процесі попереднього розгляду будемо вважати, що модуль q=2^{23}–2^{13}+1, а степінь полінома n=256. Потім генеруються

(обчислюються) випадкові вектори, тобто множини поліномів секретного ключа $\mathbf{s}_1$ і $\mathbf{s}_2$ (рядок 02) відповідно з числом поліномів k та l. Коефіцієнти цих векторів (поліномів) є елементами поля R_η, тобто з (малими) коефіцієнтами з розміром не більше η (від $-\eta$ до η). Далі з використанням матриці $\mathbf{A}$ та секретного ключа $\mathbf{s}_1$ і $\mathbf{s}_2$ обчислюється друга частина відкритого ключа $\mathbf{t}=\mathbf{A}\mathbf{s}_1+\mathbf{s}_2$ (рядок 03), а перша частина відкритого ключа задається значенням ρ. Всі алгебраїчні операції з поліномами в механізмі виконуються над кільцем полінома $R_q = \mathbb{Z}_q[X]/(X^n+1)$. Четвертий рядок показує вихідні значення відкритого P_k та секретного S_k ключів. Детально алгоритм генерації ключа наводиться в [3].

1.2. Узагальнений алгоритм вироблення ЕП

В алгоритм перевірки ЕП вводяться значення секретного ключа S_k та повідомлення M, що підписується. Далі обчислюється вектор поліномів маскування $\mathbf{y}$ з коефіцієнтами, що є меншими, ніж γ_1 (рядок 07), а також обчислюється значення вектора поліномів $\mathbf{A}\mathbf{y}$. На основі отриманого значення $\mathbf{A}\mathbf{y}$ обчислюються старші біти $\mathbf{w}_1$ ("біти високого порядку") коефіцієнтів у цьому векторі поліномів (строчка 08); $\mathbf{w}_1$ є вектором, що містить всі поліноми w_1. Потім обчислюється поліном (рядок 09) c, що є поліномом у полі R_q з точно 60 символами ±1, а решта 0. Безпосередньо ЕП обчислюється у вигляді вектора поліномів $\mathbf{z}=\mathbf{y}+c\mathbf{s}_1$.

Якщо значення ЕП $\mathbf{z}$ вивести безпосередньо після його обчислення (рядок 10), то механізм ЕП Dilithium не буде безпечним через те, що при певних значеннях секретний ключ може бути компрометований. Щоб уникнути залежності $\mathbf{z}$ від секретного ключа та його витоку, використовується відхилення вибірки. Для цього встановлюється значення параметру β як максимально можливий коефіцієнт $c\mathbf{s}_i$. Оскільки c має значення 60 ±1, а максимальний коефіцієнт в $\mathbf{s}_i$ дорівнює $\mathbf{s}_i$, то легко побачити, що $\beta \le 60\eta$. Якщо будь-який коефіцієнт $\mathbf{z}$ перевищує $\gamma_1 - \beta$, то процес ЕП відхиляється, а процедура ЕП повторюється. Також, якщо коефіцієнт бітів низького порядку вектора $\mathbf{A}\mathbf{z}-c\mathbf{t}$ більше, ніж $\gamma_2 - \beta$, то процес ЕП відхиляється, а процедура ЕП знову повторюється (рядок 11). Перша перевірка необхідна для безпеки ЕП, а інша – для його безпеки та правильності. Таким чином, процес ЕП повторюється, доти не будуть виконані дві наведені умови. Необхідно відмітити, що параметри β та γ_1 і γ_2 повинні бути вибрані, щоб очікувана кількість повторень ЕП була не надто висока (наприклад, від 4 до 7). Детально алгоритм ЕП наводиться в [3].

1.3. Узагальнений алгоритм перевірки ЕП

При перевірці ЕП перевірник обчислює $\mathbf{w}'_1$ як біти високого порядку вектора $\mathbf{A}\mathbf{z}-c\mathbf{t}$. Далі ЕП приймається, якщо всі коефіцієнти $\mathbf{z}$ менше, ніж $\gamma_1 - \beta$ і якщо c є геш-значенням повідомлення M, що перевіряється, та значення $\mathbf{w}'_1$ (рядок 13). Перевірка спрацьовує за умов, якщо

$$\text{HighBits}(\mathbf{A}\mathbf{z}-c\mathbf{t},\, 2\gamma_2) = \text{HighBits}(\mathbf{A}\mathbf{y},\, 2\gamma_2) \qquad (1)$$

Дійсно, причиною цього є те, що для дійсного ЕП буде завжди виконуватись умова

$$\|\text{LowBits}(\mathbf{A}\mathbf{y}-c\mathbf{s}_2,\, 2\gamma_2)\|_\infty < \gamma_2 - \beta. \qquad (2)$$

А так як коефіцієнти $c\mathbf{s}_2$ менше, ніж β, то додавання $c\mathbf{s}_2$ недостатньо для того, щоб викликати будь-які перенесення, збільшивши будь-який коефіцієнт низького порядку до величини, щонайменше γ_2. Таким чином, рівняння (1) є правильним, і ЕП перевіряється правильно. Детальніше ця умова розглядається нижче в розд. 4.

1.4. Загальні оцінки щодо рівня безпеки ЕП Dilithium

Якщо дотримуватись основного підходу, що викладений в [16 – 18], то безпеку механізму ЦП, що наведено на рис. 1, можна довести в моделі випадкового оракула (ROM), ґрунтуючись на складності двох проблем. Перша – це стандартна задача LWE (над кільцями поліномів), в якій пропонується відрізняти (A, t:=As_1+s_2) від (A, u), де u рівномірно випадкове. Інша проблема полягає в тому, що в [3, 18] було названо проблемою SelfTargetMSIS, тобто проблемою пошуку вектора

$$\begin{bmatrix} \mathrm{z} \\ c \\ \mathrm{v} \end{bmatrix} \tag{3}$$

з малими коефіцієнтами і повідомлення (дайджесту) μ, що задовольняє умові

$$\mathrm{H}\left(\mu \| \left[\mathrm{A} \,|\, \mathrm{t} \,|\, \mathrm{I} \right] \cdot \begin{bmatrix} \mathrm{z} \\ c \\ \mathrm{v} \end{bmatrix} \right) = c, \tag{4}$$

де A і t рівномірно випадкові, а I – одинична матриця. У ROM можна отримати (не жорстке) скорочення, використовуючи розгалужену лему [3.16] зі звичайної задачі SIS знаходження z' з малими коефіцієнтами, що задовольняють Az'=0, до SelfTargetMSIS. Можна дотримуватися цього точного підходу, щоб довести безпеку Dilithium в ROM на основі складності LWE та SIS.

У моделі квантового випадкового оракула (QROM), де зловмисник може запитувати H у суперпозиції, ситуація дещо інша. У [3, 18] було показано, що Dilithium все ще базується на LWE та SelfTargetMSIS у QROM, навіть при жорсткому скороченні, коли механізм є детермінованим. Але більше не можна безпосередньо використовувати розгалужену лему (оскільки це інший тип розгляду), щоб дати квантове скорочення від SIS до SelfTargetMSIS. Є ще вагомі підстави вважати, що задача SelfTargetMSIS, а отже, і Dilithium, є безпечною в QROM. По-перше, не існує «природних» механізмів ЕП, побудованих із Σ-протоколів, що використовують перетворення Fiat-Shamir[17], які безпечні в ROM і не безпечні в QROM. Крім того, можна встановити параметри Dilithium (залишивши структуру механізму незмінною), щоб проблема SelfTargetMSIS стала інформаційно-теоретично складною, що робить цю версію Dilithium безпечною в QROM на основі тільки LWE. Також зовсім недавно дві нові роботи ще більше звузили розрив між безпекою в ROM та QROM. Так, у [3] показано, що якщо покладений в основу Σ-протокол *руйнується*, але відрізняється особливою надійністю, то його перетворення Фіата – Шаміра є безпечним підписом в QROM.

2. Модель безпеки щодо ЕП на основі фіналіста ЕП «DILITHIUM»

Введемо поняття комплексної моделі безпеки криптографічних перетворень типу ЕП, орієнтуючись на[19 – 23]. Приймемо в якості часткових складових комплексної моделі безпеки щодо асиметричних криптоперетворень типу ЕП такі приватні моделі:

- порушника щодо асиметричних криптоперетворень типу ЕП;
- загроз щодо асиметричних криптоперетворень типу ЕП;
- безпеки щодо асиметричних криптоперетворень типу ЕП.

Нижче наводяться результати обгрунтування вказаних моделей безпеки щодо перспективних асиметричних криптоперетворень типу ЕП «DILITHIUM».

2.1. Сутність моделі порушника щодо перспективного ЕП

Побудова моделі порушника необхідна для того, щоб розробити комплекс заходів із забезпечення захищеності алгоритму. Така модель може бути побудована з урахування різних критеріїв.

По суті модель порушника – це опис можливих дій порушника, який формується на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. У якості порушника розглядається особа, що може отримати доступ до роботи з включеними до складу відповідної комп'ютерної системи засобами.

Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні таких можливостей. Класифікація є ієрархічною – кожний наступний рівень включає в себе функціональні можливості попереднього [24].

Вважатимемо, що порушник використовує усі доступні йому ресурси – найпотужніші комп'ютери і необмежний час.

Таким чином, у найгіршому випадку – порушник знає все про метод синтезу перспективного ЕП та про всі механізми безпеки, що виконуються під час синтезу та застосування, виключенням є те що криптоаналітик не знає особистого ключа чи відповідним чином обґрунтовану частину особистого ключа. У найкращому випадку порушник не знає нічого про системні параметри та ключі. У нашому випадку це рівноімовірні варіанти.

2.2. Обгрунтування та сутність моделі загроз щодо ЕП

Модель загроз ЕП (далі – Модель загроз) повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП. Відповідно до Законів інформація у основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією.

При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий [3, 29, 30]. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам інфраструктури відкритого ключа (ІВК).

Оскільки сертифікат відкритого ключа є відкритою інформацією, то під час обробки згідно з [1 – 3, 29] він повинен зберігати цілісність, справжність, доступність, неспростовність та бути захищеним від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав'язування хибного чи знищення. Усім користувачам, наприклад ІВК, має бути забезпечений доступ до ознайомлення з відкритою інформацією, в даному випадку у вигляді сертифіката відкритого ключа [29, 30].

Під час обробки (застосування) конфіденційна інформація, в нашому випадку особистий ключ, вона повинна зберігати цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, має бути практично забезпечений її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення. Тобто, безумовно має бути забезпечена конфіденційність особистого ключа кожного користувача. Також, технологічна інформація повинна бути відома тільки авторизованим на це особам та зберігати цілісність.

Таким чином, в усіх відомих додатках, у яких використовується ЕП, стосовно відкритого ключа ЕП повинне бути можливість забезпечувати його цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав'язування хибного чи знищення. Стосовно особистого ключа мають бути забезпеченими його цілісність, справжність, доступність, неспростовність та бути захищеною від несанкціонованих дій, а також повинен бути забезпеченим його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.

Тобто, як існуючі ЕП, так і перспективні ЕП, повинні дозволяти гарантовано захищати їх асиметричні пари ключів у відповідності із вказаними вище вимогами, незалежно від їх

подання при використанні – в апаратному, програмному чи апаратно-програмному вигляді. Причому, незалежно від виду їх обробки, реалізація загроз, що спрямовані на вказані ресурси, може призводити до порушення вимог безпеки первинних інформаційних ресурсів, вплинути на інше ПЗ, що підписується, та, в окремих випадках, на функціонування апаратних ресурсів.

2.3. Загальні загрози щодо ЕП

Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП був сформований з числа загроз, наявних у IT-Grundschutz Catalogues з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП.

За результатами аналізу IT-Grundschutz Catalogues щодо методів синтезу та застосування системи визначено такі загрози: атака "Людина посередині"; атака Clickjacking; викрадення даних за допомогою мобільних носіїв інформації; викрадення пристроїв, носіїв чутливої інформації та документів; витік каналами побічних електромагнітних випромінювань і наведень; відмова від дій; відмова криптомодулю; відсутнє або недостатнє оповіщення при виникненні інцидентів безпеки; відсутність дозволів для обробки персональних даних; відсутність прозорості для особи, що зацікавлена та уповноважена контролювати захист даних; відсутня або неповна документація; втрата цілісності інформації, яка повинна бути захищена; старіння криптографічних методів; зловживання повноваженнями; зловживання правами адміністратора; зловживання правами користувачів; компрометація криптографічних ключів; крадіжка чутливих даних; не виявлені інциденти інформаційної безпеки; невірне тлумачення події інформаційної безпеки; недооцінювання актуальності виправлень і змін; неналежне зберігання носіїв інформації в разі виникнення надзвичайної ситуації; необережне знищення обладнання або даних; неправильне використання криптомодулів; несанкціоноване використання криптомодулів; несанкціоноване використання прав; нестійкі криптографічні алгоритми; неякісна або відсутня автентифікація; підробні сертифікати; порушення законів або правил; проблеми при автоматизації поширення виправлень і змін; розголошення чутливої інформації; систематичний перебір паролів; троянський кінь; уразливості або помилки ПЗ; шкідливе програмне забезпечення. При синтезі та застосуванні перспективних ЕП повинне бути зроблено перекриття названих загроз.

2.4. Обгрунтування та сутність моделі безпеки щодо ЕП

В якості моделі безпеки стосовно асиметричних постквантових криптоперетворень ЕП пропонується застосовувати EUF-CMA модель [19 – 23]. EUF-CMA модель визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень. Зокрема, безпека в сенсі EUF-CMA не дозволяє криптоаналітику (зловмиснику) виробляти ЕП для повідомлень, що залежать від ключів, наприклад ЕП, при застосуванні особистого sk ключа. По суті, при застосуванні механізму безпечного ЕП, згідно з моделлю EUF-CMA ще є безпечною для EUF-CMA у випадку, коли не застосовуються запити повідомлення. Але при наявності хоча б одного запиту повідомлення, що залежить від ключів, безпека механізму ЕП порушується.

Існує два загальних формальних визначення для забезпечення безпеки схеми ЕП. Кожне з цих визначень представлено як "гра", або експеримент, який виконується між атакуючим (attacker) та деяким чесним претендентом (challenger).

Неформально експеримент EUF-CMA (екзистенційна непідроблюваність при атаці на основі підібраних повідомлень) виконується так:

1. Претендент генерує дійсну пару ключів (pk, sk) і надає pk атакуючому.

2. Атакуючий тепер може повторно запросити підписи на підібраних(вибраних) повідомленнях (M1,..., Mq) за своїм вибором, і отримує дійсні підписи (σ1,...., σq) у відповідь.

3. По завершенню експерименту зловмисник повинен вивести повідомлення та підпис M*, σ* такі, що одне повідомлення було не одним із повідомлень, які вимагали попереднього кроку (1), і (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Схема вважається безпечною, якщо жоден (ефективний) зловмисник не має ні найменшої переваги у виконанні зазначених умов. Зазвичай кількість повідомлень q обмежується лише часом дій атакуючого, однак для спеціального випадку одноразових ЕП, зловмисник обмежується запитом лише одного підпису на кроці (2).

Це визначення досить сильне, але не настільки сильне, наскільки це можливо. Дещо сильнішим визначенням є визначення та відповідна вимога SUF-CMA.

Неформально, експеримент SUF-CMA (Сильна екзистенційна непідроблюваність при атаці на основі підібраних(вибраних) повідомлень виконується так:

1. Те саме, що і в попередньому експерименті.

2. Те саме, що і в попередньому експерименті.

3. Після завершення експерименту атакуючий повинен вивести повідомлення та підпис M*, σ* такі, що (1) пара (M*, σ*) не була одним із запитаних повідомлень, а підпис повернувся на попередньому кроці, (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Атакуючий виграє, якщо вона задовольняє наведеним умовам.

1. Головна відмінність полягає в тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис. Наприклад, схема, в якій атакуючий може повторно рандомізувати дійсний підпис, щоб він залишався дійсним, але виглядав інакше, ніж вихідне значення, не задовольнила би SUF-CMA [19, 22, 23].

2. Вищезгадане визначення безпеки EUF-CMA здійснюється одноразовими схемами підпису в очевидний спосіб – єдиною модифікацією є те, що Aeuf може запитувати оракул підпису OS лише один раз. Зокрема, безпека в сенсі EUF-CMA не дозволяє зловмиснику отримувати підписи повідомлень, залежних від ключів, як підпис на повному секретному ключі sk. Фактично, враховуючи EUF-CMA-безпечну схему ЕП, легко скласти схему підписів, яка все ще є EUF-CMA-безпечною, але один запит на повідомлення, залежного від ключів, порушує безпеку схеми.

3. Огляд та аналіз атак щодо стійкості ЕП «DILITHIUM»

3.1. Класифікація атак та загальна оцінка стійкості ЕП «DILITHIUM»

В постквантовій криптології актуальними є завданнями забезпечення криптографічної стійкості щодо класичних та квантових атак. Проблема зводиться до навчання з помилками (LWE), сутність якої у наступному.

Нехай n, q є деякими натуральними числами, χ – деякий ймовірнісний розподіл над $\mathbf{Z}$ та s – секретний вектор (множина поліномів) у $\mathbf{Z}_q^n$. Ймовірнісний розподіл $L_{s,\chi}$ над $\mathbf{Z}_q^n \times \mathbf{Z}_q$ отримується обчисленням [3, 16]

$$(a,c) = (a, \langle a, s \rangle + e) \in \mathbf{Z}_q^n \times \mathbf{Z}_q, \tag{5}$$

де $a \in \mathbf{Z}_q^n$ отримується з рівномірного розподілу та $e \in \mathbf{Z}$ з розподілу χ. Атака Decision-LWE полягає у тому, щоб визначити, чи отримана пара $(a,c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ з розподілу $L_{s,\chi}$ або рівномірного розподілу. Її Search-LWE складова полягає у знаходженні s з пари $(a,c) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$. Вважається, що як проблема Decision-LWE, так і Search-LWE [3, 16] з точки зору складності є еквівалентними та можуть бути зведені одна до одної за поліноміальний час і фактично є різними поглядами на одну і ту ж задачу. Розподіл χ для цих задач зазви-

чай є дискретним нормальним розподілом над кінцевим полем з математичним очікуванням рівним 0 та дисперсією, що характеризується параметром α. При цьому більшість атак на LWE полягають у знаходженні деякого вектора v з певною нормою на решітці L з фіксованим об'ємом $vol(L)$, але з різною розмірністю m, яка фактично характеризує оптимальну кількість пар $(a_i, c_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ необхідних для атаки.

Аналіз показав, що складність проблеми навчання з помилками точно знайдена лише асимптотичне. Так, доведено [31, 32], що за певних умов складність вирішення LWE в просторі розмірності n становить щонайменше $2^{O(n)}$. Цей результат зручно використовувати для оцінки загальносистемних параметрів, проте конкретні оцінки складності криптостійкості досі не відомі. Таке пов'язано з тим, що атаки на LWE зводяться в кінцевому випадку до редукції решіток.

За останні 10 років помітний суттєвий прогрес у цьому напрямку, що призводить до постійного уточнення та зміни оцінок. Він стосується більшості сучасних криптосистем, у яких використовуються варіанти LWE над поліноміальними кільцями (PR-LWE), тобто розподіл розглядається не над $\mathbf{Z}_q$, а над $\mathbf{Z}_q[X]/(f(x))$. При аналізі криптоперетворень засобом множення використовується поліном виду $f(x) = x^{2^n} + 1$ і відповідне поле $R_q = \mathbf{Z}_q[X]/(x^{2^n} + 1)$. Причому, якщо $(a_i, c_i) \in R_q \times R_q$, то задача має назву R-LWE. Коли $(a_i, c_i) \in R_q^d \times R_q$ – M-LWE відповідно.

Відмітимо, що поліном $f(x) = x^{2^n} + 1$ обраний невипадково. Його властивості дозволяють здійснити доказ про стан захищеності асиметричного криптоперетворення щодо квантових атак. Також його властивості дозволяють використати для операцій множення поліномів швидке NTT перетворення і, як наслідок, створювати швидкодіючі реалізації криптоперетворень. Однак з теорії Галуа відомо [3, 5, 7], що поле $R_q = \mathbf{Z}_q[X]/(x^{2^n} + 1)$ має складну структуру підполів, що може бути використано для здійснення криптоаналізу. Проте, на нинішній час на практиці такі атаки носять більше обмежений теоретичний характер, ніж практичний. Фактично сучасними криптологами ігноруються додаткові можливості, а R-LWE та M-LWE розглядаються як LWE. Це пояснюється тим, що для полінома $f(x) = x^{2^n} + 1$ доведено, що R-LWE та M-LWE є складнішими за LWE атаки.

На основі аналізу визначено [33 – 41], що стосовно атак на LWE можливо виділити та необхідно розглядати наступні:

1) атака грубої сили, тобто повного перебору;
2) традиційна атака зустріч посередині;
3) атака на основі алгоритму Arora-Ge;
4) BKW, коли LWE зводиться до SIS атаки;
5) диференційні атаки на помилки на детермінований ЕП на решітках;
6) Primal attack (Search-LWE зводиться до BDD атаки);
7) Dual attack (Decision-LWE зводиться до SIS);
8) зведення до uSVP атаки пошуку короткого вектора.

Розглянемо детальніше вказані атаки та зробимо їх оцінки та порівняння. Відмітимо, що атаки 1) – 4) наведеного переліку є експоненційно складними, аналіз їх складності та можливості застосування у загальному виді наведено в [33 – 39]. Попередні оцінки дозволили зробити висновки про неможливість їх використання, оскільки їх часова та просторова складності є експоненційно складними (для випадку застосування обґрунтовано вибраних розмірах системних параметрів та ключів).

В [42] запропоновано диференційні атаки на помилки на детермінований ЕП на решітках. По суті вони зводяться до розширення застосування диференційних атак на помилки на криптографію на основі решітки. Показано, чи вразливі до таких атак дві детерміновані схеми ЕП на основі решітки – Dilithium та qTESLA. Показано, що одиничні випадкові помилки можуть спричинити сценарій повторного використання початкового стана (нонсу), який дозволяє відновити ключ. Також, зроблено розширення до атак викликаних помилками з частковим повторним використанням нонсу, які не пошкоджують дійсність обчислених ЕП тому їх важче виявити.

Використовуючи лінійну алгебру та методи зведення базису решітки, зловмисник після успішного внесення помилки може отримати один із елементів секретного ключа. Деякі інші частини ключа неможливо відновити, але показано, що алгоритм підпису з підробленим підписом все ще може успішно підписувати будь-яке повідомлення. В цій же роботі зроблено експериментальні перевірки наведених атак, наприклад виконуючи збої годинника на мікроконтролері ARM Cortex-M4 [42]. Зокрема, показано, що до 65,2 % часу виконання Dilithium вразливе до непрофільованої атаки, де випадкова помилка вводиться в будь-якому місці під час процедури підпису і все ще призводить до успішного відновлення ключа. Але, віднесемо ці можливості зловмисника до атак сторонніми каналами, їх аналіз є окремою задачею досліджень.

3.2. Атаки на основі решіток

В цьому підрозділі розглядаються такі основні атаки на основі решіток:
- із застосуванням зведення LWE до BDD атаки;
- Dual Attack зі зведенням LWE до SIS атаки;
- Primal Attack виду (LWE->uSVP);
- на основі алгоритму SIS.

3.2.1. Атака зі застосуванням зведення LWE до BDD

Сутність атаки у наступному. Припускається, що відомі m пар

$$(a_i, c_i) = (a_i, \langle a_i, s_i \rangle + e_i) \in \mathbf{Z}_q^n \times \mathbf{Z}_q .$$

Зробимо запис наведеного у більш зручному вигляді

$$(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1} . \quad (6)$$

Для (6) побудуємо решітку

$$L = \{ Ax \bmod q : x \in \mathbf{Z}_q^m \}.$$

Очевидно, що s є вектором на решітці та є найближчим до вектора $As + e$. Задача знаходження найближчого вектора на решітці до деякого довільного вектора має назву BDD та вирішується за допомогою алгоритму Бабаї [33]. Алгоритм є поліноміально складним, він працює за поліноміальний час, проте рішення знаходиться тільки з деякою ймовірністю. Для LWE цю ймовірність можна оцінити як

$$\prod_{i=0}^{m-1} erf\left(\frac{\left\| b_i^* \right\| \sqrt{\pi}}{2\alpha q} \right), \quad (7)$$

де $\left\| b_i^* \right\|$ – норми ортогоналізованих за Граммом – Шмідтом векторів базису решітки (тобто столбців матриці A). Для того щоб ймовірність вирішення BDD була близька до одиниці, потрібно зменшити $\left\| b_i^* \right\|$, тобто редукувати базис. Одним з найкращих алгоритмів для редук-

ції базиса є алгоритм блочної редукції Коркіна – Золотарьова (BKZ) та його модифікаціїї (BKZ 2.0) [38, 3]. Фактор Ерміта δ_0 для редукції можливо отримати з співвідношення

$$\begin{aligned} \left\| b_0 \right\|_2 &= \delta_0^n q^{\frac{1}{n}} \\ \left\| b_i^* \right\|_2 &\approx \delta_0^{-2i+n} * q^{\frac{1}{n}}. \end{aligned} \tag{8}$$

Алгоритм BKZ 2.0 залежить від натуральних параметрів β і m, що позначають так звані довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним – Золотарьовим базис повної решітки вимірності n за $2^{E(\beta, m, n)}$ операцій, де

$$E(\beta, m, n) = 0,000784314\,\beta^2 + 0,366078\,\beta + \log((n)m) + 0,875. \tag{9}$$

В [37] описано симулятор алгоритму BKZ 2.0, який дозволяє обчислювати за вхідним параметром $\delta_0 > 1$ такі значення параметрів β і m, що застосування алгоритму BKZ 2.0 з цими параметрами до будь-якого вхідного базису повної решітки вимірності n та приводить до її редукованого базису з кореневим фактором Ерміта δ_0.

3.2.2. Dual Attack зі зведенням LWE до SIS

Існують атаки на дуальній решітці засобом зведення LWE до SIS задачі. Сутність зведення у наступному. Побудуємо спочатку решітку $L = \{x \in \mathbf{Z}_q^m \mid A^* x = 0 \bmod q\}$. Задача SIS полягає у знаходженні такого найменшого цілого $x \in \mathbf{Z}^n$, щоб $A^* x = 0$. Припустимо, що такий вектор знайдений, тоді можна вирішити задачу Decision-LWE. Нехай дано m пар $(A, c) = (A, A^* s + e) \in \mathbf{Z}_q^{m \times n} \times \mathbf{Z}_q^{m \times 1}$. Обчислимо скалярний добуток $\langle x, c \rangle$:

$$\langle x, c \rangle = x^* a^* s + x^* e = 0^* s + x^* e = x^* e = \langle x, e \rangle. \tag{10}$$

Оскільки вектор $x \in \mathbf{Z}^n$ відомий, то з цієї рівності можна знайти значення вектора помилок *e*, проте простір помилок залишається досить великим. У [40] показано, що, якщо вектор *x* має норму

$$\left\| x \right\|_2 = \frac{1}{\alpha} * \sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}}, \tag{11}$$

то з ймовірністю близькою до 1 можливо вирішити цю задачу, при цьому знадобиться $\frac{1}{\varepsilon^2}$ запусків вирішувача SIS. Вирішувач фактично знаходить достатньо малий вектор на решітці, тобто вирішує задачу SVP. У [33] було показано, що при цьому фактор Ерміта δ_0 має бути не більше

$$\log \delta_0 = \frac{\log^2(\frac{1}{\alpha}\sqrt{\frac{\ln(\frac{1}{\varepsilon})}{\pi}})}{4 * n \log q}. \tag{12}$$

Атаки такого типу називаються Dual Attack. Точна оцінка атаки потребує вибрати певний вирішувач. У якості вирішувача можливо взяти BKZ 2.0 і виконати оцінку як для атаки на BDD.

3.2.3. Primal Attack (LWE->uSVP)

Нехай в атаці, що розглядається, решітка містить вектор *s*. Сутність Primal Attack полягає у тому, щоб побудувати таку решітку, на якій буде лежати вектор $(s,e,1)$ і він буде найменшим унікальним вектором, тобто, вона зводиться до задачі uSVP [3]. Такою решіткою буде

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}.$$

Для пошуку вектора можливо скористатися вирішувачем BKZ 2.0 і редукувати решітку, як наслідок b_0 буде рішенням, що шукається. Далі, для вдалої редукції оцінити фактор Ерміта можливо виразом [33, 40]

$$\log \delta_0 = \frac{1}{4n^2 \ln^2 q}\left(W\left((-2n\ln q) * (\sqrt{n \log q}) * \frac{(\tau\alpha)^2}{2\pi}\right)\right)^2. \quad (13)$$

3.2.4. Зауваження стосовно алгоритму SIS

Як вище вказувалось, задачу SIS можливо звести до пошуку найменшого вектора на дуальній решітці, тобто у вигляді

$$v \approx \gamma\lambda_1(L), L = \{x \in \mathbf{Z}_q^m \mid A * x = 0 \bmod q\}. \quad (14)$$

Проте, автори Dilithium запропонували інший підхід – шукати рішення як найменший вектор на решітці з обмеженням на коефіцієнти

$$v \approx \gamma\lambda_1(L), \|\gamma\lambda_1(L)\|_\infty < \beta, L = \{Ax \bmod q : x \in \mathbf{Z}_q^m\}. \quad (15)$$

Але автори не вказують, чому вони вважають такий підхід є кращим за класичний підхід.

3.3. Аналіз атаки щодо SUF-CMA безпеки

Згідно з [43] схема підпису забезпечує SUF-CMA безпеку, яка може бути визначена як

$$Adv_{Dilithium}^{SUF-CMA}(A) \le Adv_{k,l,D}^{MLWE}(B) + Adv_{H,k,l+1,\xi}^{SelfTargetMSIS}(C) + Adv_{k,l,\xi'}^{MSIS}(D) + 2^{-254}, \quad (16)$$

де D є рівномірним розподілом над відповідним полем значень,

$$\xi = \max(\gamma_1 - \beta, 2 * \gamma_2 + 1 + 2^{d-1} * h)$$

$$\xi' = \max\left(2 * [\![(\gamma]\!]_1 - \beta\right), 4 * \gamma_2 + 2),$$

тож безпека залежить від трьох атак: MLWE, SelfTargetMSIS та MSIS.

Захист від MLWE потрібен для захисту від атак на відтворення ключа. Атаки SelfTargetMSIS та MSIS направлені на підробку повідомлення. Варто зазначити, що до MLWE є дуальна атака, яка іноді може мати кращі результати. Таким чином, для удосконаленого ЕП «DILITHIUM» потрібно знайти параметри, що є стійкими до атак Primal MLWE, Dual MLWE, SelfTargetMSIS та MSIS.

У [43, 44] для оцінки безпеки застосовувалася методика “core SVP hardness”. Вона базується на тому факті, що досі не знайдено ефективних методів експлуатації структури модульних решіток, тож можна звести MLWE та MSIS до LWE та SIS без втрати точності аналізу.

Безпеку останніх можна звести до проблеми SVP, яка є добре вивченою (порівняно з іншими проблемами на решітках). Проте з кожним роком з'являються нові більш ефективні алгоритми для вирішення цієї проблеми. Найкращим відомим алгоритмом для редукції решіток є BKZ. Він мінімізує кожен вектор решітки у ортогональному підпросторі розмірності *b*. Найкраща відома складність атаки для класичних комп'ютерів складає

$$O(2^{0.292b}) \text{ та } O(2^{0.265b}) \quad (17)$$

для квантових. Під час роботи BKZ викликає "оракула" для мінімізації у ортогональному підпросторі. Найкраща відома складність оракула складає $O(2^{0.2075b})$.

3.3.1. Аналіз атаки Primal Attack

Проблема $MLWE_{k,l,D}$ зводиться до $LWE_{nk,nl,D}$, яку у свою чергу можна звести до *unique-SVP* на решітці розмірності $d = n * l + n * k + 1$. В ній норму найменшого вектора можна оцінити як $\lambda \approx \xi * \sqrt{d}$, де ξ є середньоквадратичним відхиленням для розподілу, що використовується. Оскільки в Dilithium використовується рівномірний розподіл, то $\xi = sqrt\left(\frac{\sum i^2}{2 * \eta + 1}\right)$.

Атака вважається успішною, якщо була знайдена довжина блока, для якої проекція найменшого вектора *v* у векторний простір, натягнутий на останні *b* вектори Грамма – Шмідта, коротше ніж b^*_{d-b}. Довжину вектора *v* можна оцінити як $\delta^{2*b-d-1} * q^{\frac{m}{d}}$, де $\delta = \left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)^{\frac{1}{2(b-1)}}$, а норму проекції як $\xi\sqrt{b} \le \delta^{2*b-d-1} * q^{\frac{m}{d}}$.

Алгоритм 3.1 реалізації Primal Attack наведено нижче.

Алгоритм 3.1. Primal Attack
Вхідні данні: n, q, η, l, k
Вихідні данні: криптобезпека λ_1.

bestcost = $+\infty$
for dim $\in [5, n*k]$, $b \in [50, n*k+n*l]$ {
$d = n * l + dim + 1$
$\delta = \left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)^{\frac{1}{2(b-1)}}$
$l = \delta^{2*b-d-1} * q^{\frac{m}{d}}$
$\xi = sqrt\left(\frac{\sum i^2}{2 * \eta + 1}\right)$
Якщо $\xi\sqrt{b} \le l$ та 0.296*b <bestcost, тоді bestcost = 0.296*b
}
Return bestcost

3.3.2. Аналіз атаки Dual attack

Атака Dual attack полягає у вирішенні decision–LWE на дуальній решітці. Нехай знайдено певний вектор. Якщо рішення належить до LWE, то його коефіцієнти мають мати нормальний розподіл, інакше матиме рівномірний розподіл. Відстань між нормальним та рівномірним розподілом можна оцінити як

$$\epsilon = 4\exp\left(-2*\pi^2*\left(l*\frac{\xi}{q}\right)^2\right),$$

де l – довжина вектора, ξ – середньоквадратичне відхилення. Це значення можна трактувати як ймовірність успіху. Нажаль, вона досить мала. Для успішної атаки потрібно атаку виконати щонайменше $R = \max\left(\frac{1{,}1}{2^{(0.2075*b)\epsilon^2}}\right)$ разів. Довжину вектора можна оцінити як $\delta^{d-1}*q^{\frac{n*l}{d}}$, де d – розмірність підрешітки, що обрана для атаки.

Алгоритм 3.2 реалізації Dual attack наведено нижче.

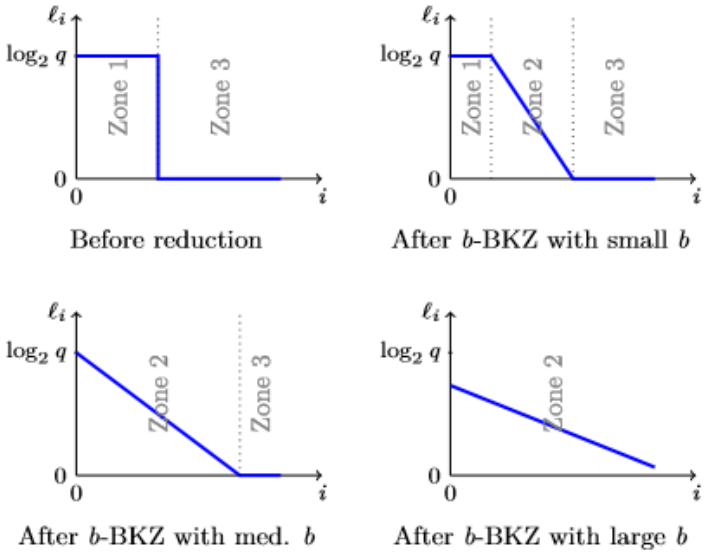
Алгоритм 3.2. Dual Attack
Вхідні параметри: n, q, k, l, η
Вихідні параметри: криптостійкість λ_2

bestcost = $+\infty$
for dim $\in [5, n*k]$, $b \in [50, n*k+n*l]$ {
$d = n*l+dim+1$
$\delta = \left((\pi*b)^{\frac{1}{b}}*\frac{b}{2*pi*e}\right)^{\frac{1}{2(b-1)}}$
$l = \delta^{d-1}*q^{\frac{n*l}{d}}$
$\xi = sqrt\left(\frac{\sum i^2}{2*\eta+1}\right)$
$\epsilon = 4\exp\left(-2*\pi^2*\left(l*\frac{\xi}{q}\right)^2\right)$
$R = \max\left(\frac{1{,}1}{2^{(0.2075*b)\epsilon^2}}\right)$
Якщо $\log_2\left(R*2^{0.2075b}\right)$<bestcost, тоді bestcost = $\log_2\left(R*2^{0.2075b}\right)$
}
Return bestcost

3.3.3. Результати застосування SIS та SelfTargetMSIS до ЕП «DILITHIUM»

У [43] було показано, що SelfTargetMSIS можна звести до MSIS, а відповідну проблему вирішення MSIS – до вирішення SIS. Задача SIS полягає у знаходженні вектору цілих чисел, які мають досить малу норму || ||. Автори пропонують шукати такий вектор за допомогою BKZ (у якому використовується $||\ ||_2$ норма). Згідно з [3, 43] після редукції решітки, що асоційована з криптосистемою ЕП «DILITHIUM», в векторах умовно можна виділити три зони. У першій зоні коефіцієнти будуть розподілені рівномірно за модулем q. У другій зоні коефі-

цієнти матимуть нормальний розподіл, а у третій зоні усі коефіцієнти дорівнюють 0. Криптостійкістю є обернена величина до добутку ймовірності того, що усі коефіцієнти менші за певне значення (що є параметром атаки) на час роботи підпроцедури, що виконує редукцію в ортогональному підпросторі із застосуванням алгоритму BKZ. Для виявлення меж зон *i, j* використовується ряд евристичних міркувань. До редукції перші вектори матимуть евклідову норму q, а останні 1. Після редукції з'явиться певний "схил". Довжина цього схили і визначатиме межі другої зони:



Згідно з [43] "крутизну схилу" можна обчислити як

$$slope(b) = -\frac{1}{b-1}\left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)$$

Алгоритм 3.3 обчислення меж зон наведено нижче.

Алгоритм 3.3. Обчислення меж зон
Вхідні данні: $b, q, q_{count}, zero_{count}$
Вихідні данні: i – кінець першої зони. j – кінець другої зони. l – довжина найбільшого вектору "на схилі".
$slope = \frac{1}{b-1}\left((\pi * b)^{\frac{1}{b}} * \frac{b}{2 * pi * e}\right)$ slope_count = $\frac{\log_2 q}{slope}$ slope_sum=slope_count*log(q)-slope*slope_count*(slope_count+1)/2 I = floor((q_count*log(q)-slope_sum)/log(q) diff = log(q)*q_count-slope_sum – i*log(q) L = log(q) +log_slope + 1.0*diff/slope_count j = i + slope_count return (i,j,L)

У [2] сказано, що рандомізація базису дозволяє зменшити складність атаки. На практиці це означає, що i=0 у алгоритмі 3.4.

Алгоритм 3.4. SIS attack
Вхідні данні: криптостійкість λ_3
Вихідні данні:
$\sigma = \frac{L}{\sqrt{J - I + 1}}$ *return* $\log_2\left(\frac{1}{p_1 * p_2 * 2^{0.207 sb}}\right)$

В розд. 4 наведено результати обчислення (генерації) системних параметрів щодо удосконаленого ЕП DILITHIUM для 128, 256, 384, 512 біт стійкості

4. Генерація загальносистемних параметрів ЕП DILITHIUM для 128, 256, 384, 512 біт стійкості

4.1. Загальні положення

Для генерації системних параметрів удосконаленого ЕП DILITHIUM використаємо результати аналізу відомих атак на криптосистему, що наведені в розд. 3, та встановимо умови, за яких забезпечується захист від них. Найочевиднішим підходом атаки криптосистеми є відновлення особистого ключа на основі використання значення відкритого ключа.

4.1.1. Атака відновлення особистого ключа на основі відкритого ключа

Як показано вище, в криптосистемі ЕП DILITHIUM вирішення цієї задачі зводиться до задачі MLWE (Module learning with errors) [43]. В літературі для аналізу MLWE використовується стратегія зведення до проблеми LWE [3, 43, 44]. З однієї сторони, це полегшує аналіз, але з іншої – залишає простір для оптимізацій. Проблема LWE може бути вирішена різними шляхами. До першого можливо віднести комбінаторні атаки, такі як BKW, Arora-Ge та зустріч посередині. Ці атаки іноді є ефективними, коли коефіцієнти полінома, що є особистим ключем, належать до деякої невеликої множини (наприклад $\{-1,0,1\}$). Як правило, їх розгляд має сенс тільки у разі гомоморфних криптосистем [3, 43]. Для ЕП DILITHIUM вони значно поступаються в ефективності і надалі розглядатися не будуть. До другої категорії належать атаки через редукцію решіток. Розглядають атаки на решітці та дуальній до неї [43]. У першому випадку будується решітка

$$\Lambda = \{x \in \mathbf{Z}^{m+n+1} : (A \mid I_m \mid -c) * x = 0 \bmod q\}. \tag{18}$$

Далі за допомогою алгоритмів редукції базису знаходиться найменший унікальний вектор (фактично задача зводиться до USVP) [44]. Для оцінки стійкості до цієї атаки зазвичай використовується підхід, що був запропонований в роботі тільки в [43]. Фактично виконується пошук найменшого розміру блоку β для BKZ, такого, що виконується умова

$$\sigma\sqrt{\beta} \le \delta_0^{2\beta-d-1} q^{\frac{n}{d}},$$

де σ, q – загальносистемні параметри, d – розмірність решітки, δ_0 – максимальне значення фактора Ерміта, за яким решітка буде достатньо редукованою. Причому δ_0 можливо вирази-

ти через β як $\delta \approx ((\pi\beta)^{\frac{1}{\beta}} * \beta / 2\pi e)^{1/2(\beta-1)}$. Таким чином, маємо нелінійне діофантове рівняння. Вирішувати його можливо повним перебором, або більш оптимізованими шляхами.

Для дуальної атаки будується решітка

$$L = \{(x, y) \in \mathbf{Z}_q^m \times \mathbf{Z}_q^n \mid A^* x = y \bmod q\} \ . \tag{19}$$

Для неї задача криптоаналітика полягає у тому, щоб визначити, чи буде знайдений після редукції вектор на цій решітці належати до розподілу, з якого отримано ключ, чи рівномірного розподілу. Згідно з [43] статистична відстань між цими двома розподілами складає $\varepsilon = 4\exp(-2\pi^2\left(\frac{l\sigma}{q}\right)^2)$, де l – довжина найменшого вектора. Відповідно, потрібно перебрати $1/\varepsilon^2$ для вдалої атаки таких векторів. Нехай вирішувач працює за час T, тоді кількість спроб можливо розрахувати як $R = \max(1, \frac{1}{T * \varepsilon^2})$. Оскільки довжина вектора l залежить від фактора Ерміта як $\delta_0^{d-1} q^{\frac{n}{d}}$, а той може бути виражений через розмір блока як

$$\delta \approx ((\pi\beta)^{\frac{1}{\beta}} * \beta / 2\pi e)^{1/2(\beta-1)},$$

то задача знову зводиться до перебору значень параметра β .

Деталізовані вище дві атаки вище називаються Primal Attack і Dual Attack відповідно і складають основу для оцінки складності криптосистем на основі LWE (та його різновидів) [43, 44]. Всі інші покращення як правило є еврістиками.

4.1.2. Атаки засобом підробки ЕП·

Іншим шляхом здійснення зловмисником атаки є підробка ЕП. У цьому разі атака здійснюється шляхом вирішення задачі SIS. Візьмемо до уваги, що дуальна атака фактично є вирішенням SIS [43, 44]. Проте автори ЕП DILITHIUM запропонували інший підхід до вирішення цієї задачі. В SIS потрібно знайти вектор, всі елементи якого менші за певну величину. Автори Dilithium пропонують шукати малі вектори на решітці до тих пір, доки всі елементи такого малого вектора не будуть менші за задану величину в задачі SIS. Нехай T – час роботи вирішувача, $p-$ ймовірність знаходження такого вектора. Тоді ймовірність атаки можливо оцінити як $\frac{1}{T * p}$. Відповідно, повторивши обчислення декілька разів, ця ймовірність зросте до потрібного рівня. Недоліком такого підходу є використання великої кількості евристичних міркувань. Проте складність оцінки криптостійкості виявляються меншою, ніж при використанні дуальної атаки. Далі, після редукції решітки в векторах умовно можна виділити, як показано вище в п. 3.3.3, три зони. У першій зоні довжини норм Грамма – Шмідта будуть розподілені рівномірно за модулем q, у другій довжини норм Грамма – Шмідта матимуть нормальний розподіл, а у третій зоні усі довжини норм Грамма – Шмідта дорівнюють 0. Якщо рандомізувати базис решітки перед редукцією, то перша зона зникає і редукція відбувається швидше.

Таким чином, потрібно, щоб перші j довжини норм Грамма – Шмідта (які розподілені за нормальним розподілом) були менші за задане значення ζ . Ймовірність цього складає

$$p = \Phi\left(\frac{\zeta}{\sigma\sqrt{2}}\right)^{j+1} \tag{20}$$

Головна проблема полягає у знаходженні необхідного значення j.

Варто окремо згадати про алгебраїчні атаки. При достатньо малих σ та достатньо великих q існують алгебраїчні атаки на LWE [45]. Для значень σ та q, що використовуються в Dilithium ці атаки не можуть бути здійснені.

4.2. Обчислення основних параметрів для удосконаленого ЕП DILITHIUM

Основні параметри для реалізації LWE та SIS атак представлені табл. 1.

Таблиця 1

Основні параметри ЕП DILITHIUM

Параметри	Значення
(N,q)	Степінь та модуль коефіцієнтів поліномів.
(k,l)	Кількість поліномів в матриці.
η	Значення коефіцієнтів особистих ключів s (знаходяться в межах $[-\eta,\eta]$.
(γ_1,γ_2)	Обмеження на максимальні значення коефіцієнтів під час вироблення підпису. Сильно впливають на стійкість до атак на підробку підпису.
β	Також впливає на максимальне значення коефіцієнтів, проте впливає не стільки на стійкість, скільки на розмір підпису. Фактично дозволяє знаходити баланс між стійкістю та техніко-економічними показниками.
d	Впливає на стійкість до атак до підробки підпису.
h	Визначає об'єм простору з якого обирається challenge
w	Впливає тільки на розмір підпису. Знаходиться з практичних міркувань.

Враховано, що чим менше N, тим швидше працюватиме схема. Автори ЕП DLILITHIUM використовують $N=256$. Збільшуючи кількість поліномів через параметри (k,l) можливо досягти будь-якого рівня стійкості до MLWE, проте для забезпечення стійкості до інших атак при використанні $N=256$ вже для рівня стійкості 384 біт не існує стійких параметрів, тому для $\lambda\in\{384,512\}$ потрібно збільшити N до 512.

Параметр q сильно впливає на стійкість. Він повинен бути простим числом. Для створення ефективних реалізацій з використанням NTT повинно виконуватися співвідношення $q\equiv 1 \bmod 2N$. Автори Dilithium використовували $q=8389417$. При збільшенні q буде знижуватися криптостійкість, немає сенсу збільшувати його значення, оскільки умова $q\equiv 1 \bmod 2N$ виконується для 256, 384, 512 біт безпеки.

Для обчислення параметрів (γ_1,γ_2) автори використовували формули

$$\gamma_1=(q-1)/16,\ \gamma_2=\gamma_1/2 \tag{21}$$

При такому виборі стійкість до всіх можливих атак буде приблизно однаковою. Такий вибір має сенс і при генерації параметрів для 256, 384, 512 біт безпеки.

Параметр h визначає кількість ненульових елементів в поліномі c. Для стійкості λ кількість можливих поліномів повинна бути не меншою за 2^λ. Тож, має виконуватися нерівність

$$2^h\binom{n}{h}\geq 2^\lambda. \tag{22}$$

Атаки на LWE можуть бути задані трьома параметрами: n, q, σ, де n – розмірність решітки (у випадку Dilithium $n = N*l+1+m, m \in \{0, N*k\}$), q – найбільше значення елементів векторів. Співпадає з значенням q в загальносистемних параметрах. σ – середньоквадратичне відхилення для розподілу, з якого отримується секретний ключ. Для ЕП DILITHIUM це значення обчислюється як

$$\sigma = \sqrt{\frac{\sum_{i=1}^{\eta} i^2}{2\eta + 1}} \tag{23}$$

Атаки на SIS параметризовано трьома параметрами: x, y, ς. Для ЕП DILITHIUM $x = N*k, y = N*l$. Параметр ζ є обмеженням на максимальне значення елементів векторів. Для ЕП DILITHIUM є дві атаки, що зводяться до SIS, тому відповідно два різних значення ζ

$$\begin{aligned} \zeta_1 &= \max(\gamma_1 - \beta, 2\gamma_2 + 1 + 2^{d-1}h) \\ \zeta_2 &= \max(2(\gamma_2 - \beta), 4\gamma_2 + 2) \end{aligned} \tag{24}$$

Якщо встановити обмеження $2^{d-1}h + 1 \le 2\gamma_2$ і врахувати що $\gamma_2 = \gamma_1/2$, то маємо:

$$\begin{aligned} \zeta_1 &\le 4\gamma_2 \\ \zeta_2 &\le 4\gamma_2 + 2 \end{aligned}. \tag{25}$$

Параметр β визначає максимальне значення коефіцієнтів поліномів $c*s_i$. Враховуючи обмеження вище, максимальне значення яке може бути отримане це $\beta = \eta h$. При такому виборі забезпечуватиметься максимальний захист від атак SIS, проте параметр β при всіх можливих значеннях майже не впливає на безпеку, тож його вплив можливо не враховувати. Проте, параметр β сильно впливає на ймовірність повтору циклу. Ця ймовірність становить

$$\approx \exp(-N\beta(\frac{l}{\gamma_1} + \frac{k}{\gamma_2})) \tag{26}$$

Тож, саме ця ймовірність є критерієм вибору параметра β.

Параметр w не впливає на криптостійкість, проте дозволяє зменшити розмір підпису ціною повтору циклу. Практичні експерименти показали, що при значенні $w = 0.08nk$ отримуються гарні результати, проте можливі подальші оптимізації.

Враховуючи приведені критерії, алгоритм генерації загальносистемних параметрів виглядає наступним чином:

1. Визначити потрібний рівень безпеки $\lambda \in \{256, 384, 512\}$;
2. Обрати значення N. Якщо $\lambda = 256$, то $N = 256$, інакше $N = 512$;
3. Обрати значення q. $q = 8389417$;
4. Обчислити γ_1 та γ_2 за формулами $\gamma_1 = (q-1)/16$, $\gamma_2 = \gamma_1/2$;
5. Обчислити значення η. За замовченням встановити $\eta = 2$. На наступних кроках значення буде уточнене;
6. Встановити значення $(k, l) = (2, 1)$;
7. Обчислити λ_1-стійкість до Primal Attack (Додаток А, алгоритм 1). Якщо стійкість менша за λ, то оновити параметри $(k, l) = (k+1, l+1)$ та повернутися до кроку 7 або збільшити η та повернутися до кроку 7;

8. Обчислити λ_2-стійкість до Dual Attack (Додаток А, алгоритм 2). Якщо стійкість менша за λ, то оновити параметри $(k,l)=(k+1,l+1)$ та повернутися до кроку 7 або збільшити η та повернутися до кроку 7;
9. Обчислити λ_3-стійкість до SIS з ζ_1 (Додаток А, алгоритм 3). Якщо стійкість менша за λ, то оновити параметри $(k,l)=(k+1,l+1)$ та повернутися до кроку 7 або збільшити $k=k+1$ та повернутися до кроку 7;
10. Обчислити λ_4-стійкість до SIS з ζ_2 (Додаток А, алгоритм 3). Якщо стійкість менша за λ, то оновити параметри $(k,l)=(k+1,l+1)$ та повернутися до кроку 7 або збільшити $k=k+1$ та повернутися до кроку 7;
11. Обчислити h як найбільше ціле, для якого виконується нерівність $2^h\binom{n}{h}\geq 2^{\lambda}$;
12. Обчислити d як найбільше ціле, для якого виконується нерівність $2^{d-1}h+1\leq 2\gamma_2$;
13. Встановити $\beta=\eta h$ та зменшувати β, щоб ймовірність повтору циклу була достатньо малою;
14. Обчислити $w=0.08nk$ (цей крок не впливає на криптостійкість та його можливо оптимізувати).

В табл. 2 наведено значення параметрів для удосконаленого ЕП DILITHIUM.

Таблиця 2

Значення параметрів для 256, 384, 512 біт стійкості

Набір	N,q	γ_1	γ_2	k,l	η	β	d	h	ω
256	(256,8380417)	523776	261888	(9,8)	2	144	14	60	184
384	(512, 8380417)	523776	261888	(7,5)	5	100	13	77	286
512	(512, 8380417)	523776	261888	(9,8)	2	74	13	118	368

Ймовірність повтору циклу при цьому складає для 256 біт – 0,15442678312246608, для 384 біт – 0,15609624568669475 і для 512 біт – 0,15247678668181552

Результати оцінки криптостійкості для удосконаленого ЕП DILITHIUM (в бітах) з використанням параметрів з табл. 2 наведено в табл. 3.

Таблиця 3

Оцінки криптостійкості для удосконаленого ЕП DILITHIUM

Набір	Primal Attack (класичний)	Primal Attack (квантовий)	Dual Attack (класичний)	Dual Attack (квантовий)	SIS (класичний)	SIS (квантовий)
256	298	270	296	269	293	266
384	440	399	438	397	503	456
512	582	527	579	525	590	535

Висновки

1. Наразі спостерігається стійкий прогрес у створенні квантових комп'ютерів. Практично завершується створення математичних основ та програмного забезпечення для таких квантових комп’ютерів. Розробляються квантові комп'ютери, що призначаються для криптоаналізу

існуючих стандартизованих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення. Національний інститут стандартів і технологій (NIST) США закінчив та прийняв рішення у вигляді проєкту стандарту NIST 8309 щодо 2-го раунду конкурсу на перспективні стандартні алгоритми електронного (цифрового) підпису (ЕП). Його підсумком є визначення фіналістів другого етапу конкурсу у вигляді проєктів CRYSTALS-DILITHIUM, FALCON та Rainbow [2, 3]. Також визначені три альтернативних кандидатів, які потребують більш детальних досліджень уже на четвертому етапі конкурсу – GeMSS, Picnic та SPHINCS+.

2. Одним із основних проблемних питань, що потрібно вирішувати є обґрунтування необхідності та розробки удосконаленої версії ЕП Dilithium, що може забезпечувати в постквантовий період 128, 256, 384 і 512 біт безпеки проти класичного та 64, 128, 192 та 256 біт проти квантового криптоаналізу від найбільш загрозливих атак [2, 16 – 18].

3. Метод (схема) ЕП Dilithium ґрунтується на підході, що отримав назву "Fiat-Shamir з перериваннями. Він в певній мірі схожий на схему, що запропонована з послідовним удосконаленням в [16, 17]. В перспективі необхідно вирішувати проблему обчислення (генерування) системних параметрів для удосконаленого ЕП Dilithium.

4. В якості часткових складових комплексної моделі безпеки щодо асиметричних криптоперетворень типу ЕП прийнято та визначено такі приватні моделі:

- модель порушника щодо асиметричних криптоперетворень типу ЕП;
- модель загроз щодо асиметричних криптоперетворень типу ЕП;
- модель безпеки щодо асиметричних криптоперетворень типу ЕП.

5. Отримані результати дозволяють зробити висновок, що атаки на LWE можливо розділити на два великі класи – атаки, що ґрунтуються на переборі, та атаки, що ґрунтуються на редукції решіток. До першого класу належать атаки повного перебору, зустріч посередині та Arora-Ge. Підхід, що використаний в атаці Arora-Ge, є цікавим та перспективним, але він поки що поступається атакам на решітках.

6. Попередній аналіз дозволяє зробити висновок, що сучасні варіанти механізмів LWE ґрунтуються на поліноміальних кільцях, зокрема на $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$. Властивості поліномів кільця дозволяють довести ряд теоретичних тверджень щодо стійкості криптосистеми і розробляти ефективні програмні реалізації. Проте, такі кільця мають нетривіальні підполя, що теоретично може використовуватися для криптоаналізу, проте на практиці атак, що застосовують ці додаткові структури, не було знайдено, або ці атаки знаходяться в незавершеному вигляді досліджень.

7. Проблеми криптоаналізу RLWE та MLWE по суті зводяться до LWE проблеми. Таке зведення можливо для $R_q = \mathbf{Z}_q[X]/(x^{2^n}+1)$, оскільки доведено, що RLWE є не менш стійким, ніж LWE. Проте, при такому підході внутрішня структура кільця ігнорується.

8. Атаки на решітках полягають у зведенні проблеми LWE до достатньо вивчених теоретичних проблем в теорії решіток. Існують три основні підходи: зведення LWE до BDD, зведення LWE до SIS, зведення LWE до SVP. Кожен з цих підходів в кінцевому випадку зводиться до задачі пошуку достатньо малого вектора на решітці, для чого використовується алгоритм BKZ та його варіації.

9. Точні оцінки для BKZ та його варіацій невідомі. При практичній оцінці використовується ряд евристичних підходів та екстраполяція результатів, що отримані на решітках меншої розмірності. Це становить основну проблему при оцінці криптостійкості систем подібних Dilithium, оскільки немає гарантії, що не з'явиться кращий спосіб редукції решіток, або оцінка виявиться недопустимо неточною.

10. Для генерації системних параметрів удосконаленого ЕП DILITHIUM використаємо результати аналізу відомих атак на криптосистему, що наведені в розд. 3, та встановимо умо-

ви, за яких забезпечується захист від них. Найочевиднішим підходом атаки криптосистеми є відновлення особистого ключа на основі використання значення відкритого ключа.

11. Деталізовані дві атаки називаються Primal Attack і Dual Attack відповідно і складають основу для оцінки складності криптосистем на основі LWE (та його різновидів) [43, 44]. Всі інші покращення як правило є евристиками.

12. Атака підробки ЕП· здійснюється шляхом вирішення задачі SIS. Візьмемо до уваги, що дуальна атака фактично є вирішенням SIS. Проте автори ЕП DILITHIUM запропонували інший підхід до вирішення цієї задачі. В SIS потрібно знайти вектор, всі елементи якого менші за певну величину. Автори Dilithium пропонують шукати малі вектори на решітці до тих пір, доки всі елементи такого малого вектора не будуть менші за задану величину в задачі SIS.

13. Враховано, що чим менше N, тим швидше працюватиме схема. Автори ЕП DLILITHIUM використовують $N = 256$. Збільшуючи кількість поліномів через параметри, (k,l), можливо досягти будь-якого рівня стійкості до MLWE, проте для забезпечення стійкості до інших атак при використанні $N = 256$ вже для рівня стійкості 384 біт не існує стійких параметрів, тому для $\lambda \in \{384,512\}$ потрібно збільшити N до 512.

14. В табл. 2, 3 наведені значення параметрів та оцінки криптостійкості для удосконаленого ЕП DILITHIUM з рівнями безпеки 256, 384, 512 біт.

Список літератури:

1. Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner RA, Smith-Tone D (2016) Report on Post-Quantum Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8105. https://doi.org/10.6028/NIST.IR.8105.
2. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
3. ЕП Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehlé CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation. Access mode: https://pq-crystals.org/dilithium/data/dilithium-specification.pdf.
4. Post-Quantum Cryptography. Round 2 Submissions. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.
5. 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.
6. ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2019. 445 p.
7. Gorbenko Ivan The problem of cryptographic transformations standardization and the state of its solution / Ivan Gorbenko, Olena Kachko, Oleksandr Kuznetsov, Yurii Gorbenko, Maryna Yesina // VII Міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем" : Праці Науково-технічної конференції, 30–31 травня 2019 р. Львів : Нац. ун-т "Львівська політехніка", 2019. С. 84-85.
8. Горбенко І. Д. Порівняння, оцінювання, дослідження можливості використання та переваг постквантових алгоритмів / І. Д. Горбенко, В. А. Пономар, М. В. Єсіна // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ : Нац. техн. ун-т України "Київський політехнічний інститут імені Ігоря Сікорського", 2017. Вип. 2(34). С. 9-32.
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. Квантовые компьютеры. [Електронний ресурс]. Режим доступу: http://www.nkj.ru/archive/articles/5309/.
11. Горбенко І. Д., Постквантова криптографія та механізми її реалізації / І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, Ю. І. Горбенко, Р. С., Ганзя, В. А. Пономар // Радиотехника. 2017. Вып. 186. С. 32–52.
12. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. [Електронний ресурс]. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056.
13. Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In ASIACRYPT, pages 598–616, 2009.

14. Vadim Lyubashevsky. Lattice signatures without trapdoors. In EUROCRYPT, pages 738–755, 2012.
15. Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In CHES, pages 530–547, 2012.
16. Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. Cryptology ePrint Archive, Report 2017/916, 2017. Access mode: https://eprint.iacr.org/2017/916.
17. Lyubashevsly V (2009) Fiat-Shamir with aborts: Applications to Lattice and Factoring-Based Signatures. International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT (Springer), pp. 598-616. https://doi.org/10.1007/978-3-642-10366-7_35.
18. Don J, Fehr S, Majenz C, Schaffner C (2019) Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model. Annual International Cryptology Conference – CRYPTO (Springer), p. 356-383. https://doi.org/10.1007/978-3-030-26951-7_13.
19. Єсіна М. В. Моделі безпеки постквантових криптографічних примітивів / М. В. Єсіна // Міжнародний науковий симпозіум "Питання оптимізації обчислень (ПОО-XLVI)", 2019 р. Математичне на комп'ютерне моделювання. Серія: Технічні науки. Вип. 19. С. 49-55.
20. V. Shoup On Formal Models for Secure Key Exchange, Theory of Cryptography Library, 1999. [Електронний ресурс]. Режим доступу: http://philby.ucsd.edu/cryptolib/1999/9912.html.
21. M. Bellare, R. Canetti, H. Krawczyk A modular approach to the design and analysis of authentication and key-exchange protocols. 30th STOC 1998.
22. Privacy for Code-Based Encryption in the Standard Model. In: Lange T., Takagi T. (eds) Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, vol 10346. Springer, Cham.
23. M. Bellare, A. Boldyreva, A. Desai, D. Pointcheval Key-privacy in public-key encryption. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248. P. 566–582. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1.
24. Державна служба спеціального зв'язку та захисту інформації України. Наказ від 20.07.2007 №141 «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної та відкритої інформації з використанням електронного цифрового підпису» № 862/14129.
25. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403.
26. Закон України «Про електронні довірчі послуги» // Відомості Верховної Ради (ВВР), 2017. № 45. Ст. 400).
27. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
28. Закон України "Про захист персональних даних.
29. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем : монографія. Харків : Форт, 2015. 959 с.
30. Горбенко І. Д. Прикладна криптологія: Монографія / Горбенко І. Д., Горбенко Ю. І. 2-ге вид. Харків : Форт, 2012. 868 с.
31. Albrecht M.R., Goepfert F., Virdia F., Wunderer T. Revisiting the expected cost of solwing uSVP and applications to LWE // Cryptology ePrint Archive, Report 2017/815. Access mode: http://eprint.iacr.org/2017/815.
32. Albrecht M.R., Player R., Scott S. On the concrete hardness of learning with errors // Cryptology ePrint Archive, Report 2015/046. Access mode: http://eprint.iacr.org/2015/046.
33. Rachel Player Parameter selection in lattice-based cryptography. Access mode: https://pure.royalholloway.ac.uk/portal/files/29983580/2018playerrphd.pdf.
34. Gottfried Herold, Elena Kirshanova and Alexander May. On the asymptotic complexity of solving LWE // Designs, Codes and Cryptography, Jan 2017.
35. Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE // Willy Susilo and Yi Mu, editors, ACISP 14, vol. 8544 of LNCS, pages 322–337. Springer, Heidelberg, July 2011.
36. Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors // Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, ICALP 2011, Part I, vol. 6755 of LNCS, pages 403–415. Springer, Heidelberg, July 2011.
37. Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret. Algebraic algorithms for LWE. Cryptology ePrint Archive, Report 2014/1018, 2014. Access mode: http://eprint.iacr.org/2014/1018.
38. Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the BKW algorithm on LWE // Designs, Codes and Cryptography, 74:325–354, 2015.
39. Martin R. Albrecht, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. Lazy modulus switching for the BKW algorithm on LWE // Hugo Krawczyk, editor, PKC 2014, vol. 8383 of LNCS, pages 429–445. Springer, Heidelberg, March 2014.
40. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption // Aggelos Kiayias, editor, CT-RSA 2011, vol. 6558 of LNCS, pages 319–339. Springer, Heidelberg, February 2011.
41. Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model // Journal of the ACM, 50(4): 506–519, July 2003.
42. Leon Groot Bruinderink1 and Peter Pessl2 . Differential Fault Attacks on Deterministic Lattice Signatures.

43. Lyubachevsky V., Ducas L., Kiltz E. [et all]. CRYSTALS–Dilithium. Techn. rep. NIST (2017). [Electronic resource]. Access mode: https://crc.nist.gov./projects/post-quantum-cryptogtraphy/ round-1-submissions.

44. Albrecht M.R., Goepfert F., Virdia F., Wunderer T. Revisiting the expected cost of solwing uSVP and applications to LWE // Cryptology ePrint Archive, Report 2017/815. Access mode: http://eprint.iacr.org/2017/815.

45. Peikert C., How (not) to instanaite Ring-LWE // Cryptology ePrintAchive 2016/351, 2016.

46. Горбенко І. Д. Особливості побудування та аналіз електронних підписів 5 рівня безпеки для постквантового періоду на основі алгебраїчних решіток / І. Д. Горбенко, О. Г. Качко, А. М. Олексійчук, Ю. І. Горбенко, В. П. Звєрєв, М. В. Єсіна, В. А. Пономар // Прикладная радиоэлектроника. Харьков : ХНУРЭ, 2019. Т. 18, № 3, 4. С. 123–136.

Надійшла до редколегії 05.08.2020

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, головний конструктор АТ «Інститут інформаційних технологій», Україна, e-mail: GorbenkoI@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Олексійчук Антон Миколайович – д-р техн. наук, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "КПІ", професор спеціальної кафедри №1, Україна, ORCID: https://orcid.org/0000-0003-4385-4631

Качко Олена Григорівна – канд. техн. наук, Харківський національний університет радіоелектроніки, професор кафедри програмної інженерії, начальник відділу програмування АТ «Інститут інформаційних технологій», Україна, e-mail: iit@iit.kharkov.ua, ORCID: https://orcid.org/0000-0001-9249-0497

Горбенко Юрій Іванович – канд. техн. наук, АТ «інститут інформаційних технологій», перший заступник головного конструктора, Україна, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, старший викладач кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Кандій Сергій Олександрович - Харківський національний університет імені В.Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: kandy.sergey@yandex.ua