УДК 004.056.5 **DOI:10.30837/rt.2022.3.210.06**

Є.В. ОСТРЯНСЬКА, М.В. ЄСІНА, канд. техн. наук, І.Д. ГОРБЕНКО, д-р техн. наук

АНАЛІЗ ПОГЛЯДІВ ЄВРОПЕЙСЬКОГО СОЮЗУ НА КВАНТОВО-ПОСТКВАНТОВІ ОБМЕЖЕННЯ

Вступ

Практично всім асиметричним криптографічним схемам, які зараз використовуються, загрожує потенційна розробка потужних квантових комп'ютерів. Постквантова криптографія є одним із способів боротьби з цією загрозою. Її безпека базується на складності математичних проблем, які наразі вважаються нерозв'язними ефективно – навіть за допомогою квантових комп'ютерів.

Однак із розробкою потужного квантового комп'ютера, на якому можна використовувати алгоритми Шора, безпека криптографії з відкритим ключем, яка використовується сьогодні, у майбутньому опиниться під серйозною загрозою. Це також впливає на типові схеми узгодження ключів, що є важливим елементом для захисту конфіденційності даних. Особливо це стосується даних, які повинні бути конфіденційними протягом тривалого періоду часу. Наприклад, якщо сьогодні зловмисник зафіксує обмін ключами, цілком можливо, що в майбутньому, коли стануть доступними криптографічно релевантні квантові комп'ютери, криптоаналітик зможе обчислити спільний ключ, розшифрувати та прочитати дані, зашифровані ним. Цей сценарій також відомий як «зберегти зараз, розшифрувати пізніше».

Щоб протистояти загрозі сучасної асиметричної криптографії з боку квантових комп'ютерів, виникла нова галузь криптографічних досліджень: постквантова криптографія.

Постквантова криптографія займається розробкою та дослідженням асиметричних криптосистем, які, згідно з сучасними знаннями, не можуть бути зламані навіть потужними квантовими комп'ютерами. Ці методи базуються на математичних задачах, для розв'язання яких на сьогодні невідомі ані ефективні класичні алгоритми, ані ефективні квантові алгоритми. У сучасних дослідженнях застосовуються різні підходи до реалізації постквантової криптографії, серед них: криптографія на основі кодів, криптографія на основі решітки, криптографія на основі гешування, криптографія на основі ізогенії та багатовимірна криптографія.

Метою статті є огляд обчислювальної моделі квантових комп'ютерів; квантових алгоритмів, які найбільше впливають на сучасну криптографію; ризику створення криптографічно-релевантних квантових комп'ютерів (CRQC); безпеки симетричної криптографії та криптографії з відкритим ключем за наявності CRQC; зусилля зі стандартизації NIST PQC; перехід до квантово-стійкої криптографії з відкритим ключем; актуальність та поточний стан розвитку квантово-стійкої криптографії у Європейському Союзі. Також висвітлюється хід найважливіших зусиль у цій галузі: стандартизації постквантової криптографії NIST.

1. Попередні визначення квантово-безпечної криптографії

Квантово-стійка криптографія – це криптографія, яка спрямована на надання криптографічних функцій і протоколів, які залишаються безпечними, навіть, якщо створено великомасштабні відмовостійкі квантові комп'ютери [1]. В останні роки спостерігається стійкий прогрес у створенні квантових комп'ютерів. У разі реалізації великомасштабних квантових комп'ютерів вони будуть загрожувати безпеці багатьох широко використовуваних криптосистем з відкритим ключем. Схеми встановлення ключів і цифрові підписи, засновані на факторизації, дискретних логарифмах і криптографії на еліптичних кривих, найбільш сильно постраждають. Симетричні криптографічні примітиви, такі як блокові шифри і геш-функції, будуть порушені незначно. Як результат, було проведено активізацію досліджень щодо пошуку криптосистем на відкритих ключах, які були б захищені від зловмисників як з квантовими, так і з класичними комп'ютерами. Цю область часто називають постквантовою криптографі-

єю (PQC), або іноді квантово-стійкою криптографією. Мета полягає в розробці схем, які можна розгорнути в існуючих комунікаційних мережах та протоколах без суттєвих змін.

2. Перспектива розвитку та загроза квантових комп'ютерів

Наразі немає однозначної відповіді та дуже незрозуміло, коли і навіть, якщо CRQC колинебудь буде побудовано. Розрив між сучасними квантовими комп'ютерами та передбачуваними CRQC величезний, і галузь стикається з деякими найближчими проблемами, такими як, наприклад, відсутність відомих програм для квантових комп'ютерів Noisy Intermediate-Scale (NISQ), які, як очікується, будуть створені найближчими роками.

Найкраща поточна оцінка, яка є на даний час, полягає в тому, що комітет експертів у 2019 році дійшов висновку, що поява CRQC протягом наступного десятиліття буде дуже несподіваною.

Колективні зусилля, спрямовані на створення квантових комп'ютерів, які можуть виконувати великі алгоритми, є широкими та складними. Є кілька публічно відомих залучень як в наукових колах, так і в промисловості [2, 3]. Існує також безліч потенційних реалізацій квантового комп'ютера (наприклад, з точки зору того, як реалізувати фізичні кубіти та квантові вентилі), які вивчаються та пропонуються, з надпровідними кубітами та кубітами на основі захоплених іонів, які є популярними кандидатами. Однак існує величезна різниця між сучасними гучними маленькими квантовими комп'ютерами та передбачуваними CRQC [4]. Так, на рис. 1 зображено передбачувану структуру майбутніх квантових комп'ютерів з виправленням помилок.

Рис. 1. Передбачувана структура майбутніх квантових комп'ютерів з виправленням помилок

Остання та найкраща оцінка, яка є на даний момент часу, полягає в тому, що комітет експертів з наукових кіл та промисловості у звіті 2019 року дійшов висновку, що поява CRQC протягом наступного десятиліття буде дуже несподіваною [4]. У тому ж звіті стверджується, що немає жодних відомих практичних застосувань для квантових комп'ютерів із шумовим проміжним масштабом (NISQ), які можна побачити в найближчі роки. У звіті також стверджується, що в іншому випадку галузь створення квантових комп'ютерів може стати суворо залежною від державного фінансування, якщо в найближчому майбутньому не вдасться знайти корисні програми.

Крім технічних аргументів і аргументів щодо зручності використання, оцінка прогресу квантових комп'ютерів ще більше ускладнюється іншими аспектами. По суті, те, що роблять учасники спільноти безпеки (тобто промисловість, наукові кола, уряди та організації зі стандартизації), це спостерігають один за одним, щоб оцінити, як інші учасники оцінюють ризик. Тоді ми можемо зауважити, що спільнота безпеки в цілому, здається, спокійно очікує результатів стандартизації NIST PQC, яка обговорюється в розд. 3 [5].

Щоб оцінити, коли буде необхідний перехід до квантово-безпечної криптографії, дуже показовим є наступне міркування фізика-теоретика M. Mosca з [6], що схематично зображено на рис. 2.

Нехай:

- x – кількість років, протягом яких дані, що підлягають захисту, повинні залишатися в безпеці,
- y – кількість років, необхідних для перетворення відповідної системи на стійку до квантового комп'ютера криптографію,
- z – кількість років, які знадобляться для існування квантових комп'ютерів, які загрожують криптографії, яка зараз використовується.

Тоді, якщо $x+y>z$, у вас проблема!

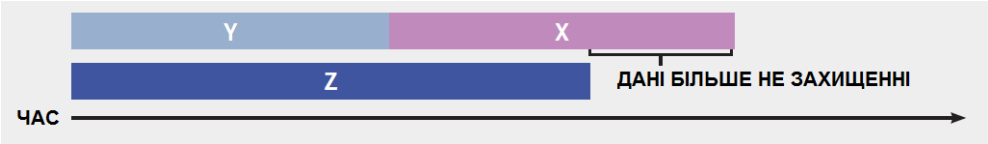

Рис. 2. Зображення «Теореми Mosca»

Це твердження стало відомим як «теорема Mosca», хоча це, звичайно, досить очевидне твердження.

Якщо перехід до квантово-безпечної криптографії розпочати сьогодні, він завершиться через y років. Наскільки великий y, залежить від різних факторів, таких як ступінь впливу на системи та доступність квантово-безпечних альтернатив. Отже, важливим першим кроком є оцінка та розробка плану міграції [7].

Таким чином, останні дані, які все ще були зашифровані за допомогою старих методів, будуть згенеровані через y років, а потім мають бути захищені ще на x років. У випадку спілкування в реальному часі цей період часу x може бути зникаюче малим. Натомість, наприклад, конфіденційна медична інформація має залишатися в безпеці протягом кількох десятиліть.

Припустимо, що виконується $x+y>z$. Потім можна перехопити останні дані, які ще не захищені квантово-безпечним способом, і розшифрувати їх протягом часу, протягом якого вони повинні бути захищені. Таким чином, перехід до квантово-безпечної криптографії має розпочатися досить рано, щоб $x+y<z$ все ще витримувався для всіх даних, які потрібно захистити. Але залишається під питанням наскільки великим має бути z.

Для національних систем безпеки BSI працює згідно з гіпотезою, що криптографічно відповідні квантові комп'ютери будуть доступні на початку 2030-х років [9, 10]. Слід підкреслити, що це твердження не слід розуміти як прогноз доступності квантових комп'ютерів, а скоріше представляє еталон для оцінки ризику. Тому BSI ініціював перехід до квантово-безпечної криптографії відповідно до програми федерального уряду «Квантові технології – від фундаментальних досліджень до ринку» [11].

3. Стандартизація постквантової криптографії

Постквантова криптографія займається розробкою та дослідженням асиметричних криптосистем, які, згідно з сучасними знаннями, не можуть бути зламані навіть потужними квантовими комп'ютерами. Ці методи базуються на математичних задачах, для розв'язання яких на сьогодні невідомі ані ефективні класичні алгоритми, ані ефективні квантові алгоритми. У сучасних дослідженнях застосовуються різні підходи до реалізації постквантової криптографії. До них належать, серед іншого:

- Криптографія на основі кодів: безпека схем на основі кодів ґрунтується на труднощах ефективного декодування загальних кодів з виправленням помилок.
- Криптографія на основі решітки: безпека схем на основі решітки базується на складності вирішення певних обчислювальних проблем на математичних решітках.

- Криптографія на основі гешування: безпека схем підпису на основі гешування базується на властивостях безпеки використаної геш-функції.
- Криптографія на основі ізогенії: схеми на основі ізогенії базують свою безпеку на тому факті, що важко знайти ізогенію між двома суперсингулярними еліптичними кривими, якщо така існує.
- Багатовимірна криптографія: безпека багатовимірної криптографії базується на припущенні, що багатовимірні поліноміальні системи рівнянь над скінченними полями важко вирішити.

Далі в цьому розділі будуть розглянуті лише перші три класи, оскільки постквантові схеми, рекомендовані BSI, належать лише до цих класів. Багатовимірні схеми мають довгу історію атак і виправлень. В даний час BSI не має наміру рекомендувати використання багатовимірних схем. Криптографія, заснована на ізогеніях (відображення між еліптичними кривими зі спеціальними властивостями), є цікавою темою дослідження, яку, на думку BSI, слід вивчити далі, перш ніж розглядати рекомендацію.

Як було вже наголошено, в останні роки постквантова криптографія набула значного значення: у серпні 2015 року Агентство національної безпеки США (NSA) попередило про вплив квантових комп'ютерів на безпеку криптографічних схем та ініціювало перехід на постквантові криптосистеми. Як виправдання NSA посилалося на досягнення у фізиці та технологіях, які могли б дозволити розробити криптографічно відповідний квантовий комп'ютер. NSA не назвало жодних конкретних постквантових алгоритмів, але послалося на майбутні стандарти Національного інституту стандартів і технологій (NIST).

Згідно з повідомленням NSA, NIST розпочав процес у листопаді 2016 року, наприкінці якого має бути доступний вибір постквантових схем. Цей процес проводиться в кілька раундів. До кінцевого терміну подання в листопаді 2017 року було подано 82 пропозиції, з яких 69 відповідали мінімальним критеріям і були прийняті NIST як кандидати в першому раунді. У січні 2019 року на основі публічних коментарів дослідницького співтовариства та внутрішнього аналізу NIST відібрав 26 із цих кандидатів для проходження до 2-го туру. Ці 26 кандидатів 2-го туру включають 17 схем асиметричного шифрування або узгодження ключів і 9 схем цифрових підписів. Потім, у липні 2020 року, NIST оголосив кандидатів, які пройдуть до 3-го туру. NIST розділив кандидатів 3-го туру на «фіналістів» і «альтернативних кандидатів». Причини, чому деякі схеми були названі альтернативними кандидатами, дуже різні.

Після трьох раундів оцінки та аналізу, NIST вибрав перші алгоритми, які він стандартизує в результаті процесу стандартизації PQC. Механізм інкапсуляції відкритого ключа (KEM), який буде стандартизований, – Crystals-Kyber. Цифрові підписи, які будуть стандартизовані, – Crystals-Dilithium, Falcon, та Sphincs+. Незважаючи на те, що вибираються кілька алгоритмів підпису, NIST рекомендує Crystals-Dilithium як основний алгоритм, який повинен бути реалізований. Крім того, чотири альтернативні алгоритми-кандидати KEM проходять до 4-го раунду оцінки: BIKE, Classic McEliece, HQC та SIKE. Ці кандидати будуть розглянуті для майбутньої стандартизації після завершення 4-го раунду.

Через терміновість переходу на процедури узгодження ключів, стійкі до квантового комп'ютера, BSI вперше рекомендував дві з цих схем у своїй технічній настанові TR-02102-1 [12] ще на початку 2020 року. У той же час німецька крипто індустрія має надію, що це має надати орієнтацію та дозволити їй розробляти продукти, готові до ринку, на ранній стадії, і це допоможе BSI зосередити дослідження безпеки на відповідних алгоритмах. Ці дві схеми – FrodoKEM [13] на основі решітки та Classic McEliece на основі коду [14], обидві з яких на той час перебували у 2-му раунді процесу NIST. У той час як Classic McEliece зараз є серед фіналістів 3-го раунду, FrodoKEM був включений до списку альтернативних кандидатів.

Паралельно з процесом NIST, а також у контексті постквантової криптографії, існують інші види стандартизації. Наприклад, Китайська асоціація криптологічних досліджень (CACR) проводила національний конкурс з 2018 по 2019 рік.

BSI вітає процес NIST як метод визначення стандартів у прозорому міжнародному процесі, який потім можна використовувати в усьому світі. Це особливо відноситься до окремого процесу стандартизації німецьких або європейських алгоритмів. «Поширення» міжнародних стандартів перешкоджатиме сумісності та зменшить ринкові можливості виробників криптовалюти. Крім того, розподіл персоналу та дослідницьких ресурсів призведе до нижчої якості оцінювання тих алгоритмів, які в кінцевому підсумку будуть обрані.

3.1. Транспортування ключів

Процес NIST спочатку шукав методи як для транспортування ключів, так і для шифрування. Однак стало очевидним, що подання, по суті, зосереджувалися на транспортуванні ключів і визначали асиметричне шифрування лише як попередній етап для такого механізму. В основному йдеться про методи FrodoKEM і Classic McEliece, рекомендовані BSI. FrodoKEM – це схема транспортування ключів на основі решітки, безпека якої базується на припущенні, що так звану проблему навчання з помилками (LWE) важко вирішити для класичних і квантових комп'ютерів. На відміну від багатьох інших схем на основі решіток у процесі NIST, базові решітки FrodoKEM не мають додаткової алгебраїчної структури. Хоча невідомо, чи така додаткова структура може бути використана криптоаналітиками, FrodoKEM таким чином усуває цей ризик. З іншого боку, FrodoKEM є дещо неефективним порівняно з деякими іншими схемами транспортування ключів на основі решітки. Додаткову інформацію про FrodoKEM також можна знайти в [15]. NIST виправдовує рішення включити FrodoKEM до списку альтернативних кандидатів тим, що хоча FrodoKEM має потенційні переваги в безпеці перед іншими схемами на основі решітки, він також пропонує нижчу продуктивність. Таким чином, стандартизація FrodoKEM, швидше за все, може почекати до закінчення 3-го раунду, і FrodoKEM також може служити «консервативною резервною копією», якщо криптоаналітичні досягнення будуть досягнуті щодо решіток з додатковою алгебраїчною структурою. Оскільки причина, по якій FrodoKEM не було включено до списку фіналістів 3-го раунду, не стосується безпеки схеми, BSI продовжує дотримуватися своєї рекомендації FrodoKEM.

Класичний McEliece – це схема транспортування ключів на основі коду, заснована на варіанті Niederreiter [16] схеми шифрування McEliece [17], створеному за допомогою двійкових кодів Гоппи. Оригінальна криптосистема McEliece була представлена ще в 1978 році, тому вона має довгу історію незламування порівняно з іншими постквантовими криптосистемами. Одним із недоліків схеми є те, що вона вимагає дуже великих відкритих ключів порівняно з іншими кандидатами, що може зробити її використання проблематичним у деяких сценаріях.

Таблиця 1

Середня продуктивність одноядерного процесора на Intel Xeon E-2124 3,3 ГГц для деяких кандидатів на алгоритм NIST PQC KEM (і деяких поточних альтернатив, не пов'язаних з PQC) на рівні безпеки 1 NIST PQC

Алгоритм KEM	Генерація ключа	Інкапсуляція	Декапсуляція	Розмір відкритого ключа	Розмір інкапсуляції
NTRU (ntruhps2048509)	0.048 ms	0.0073 ms	0.012 ms	699 B	699 B
Kyber (kyber512)	0.0070 ms	0.011 ms	0.0084 ms	800 B	768 B
SABER (lightsaber2)	0.012 ms	0.016 ms	0.016 ms	672 B	736 B
Classic McEliece (mceliece348864)	14 ms	0.011 ms	0.036 ms	261120 B	128 B
SIKE (SIKEp434_compressed)	3.0 ms	4.4 ms	3.3 ms	197 B	236 B
ECDH (X25519) (non-PQC)	0.038 ms	0.044 ms	0.044 ms	32 B	32 B
ECDH (P-256) (non-PQC)	0.074 ms	0.18 ms	0.18 ms	32-64 B	32-64 B
RSA-3072 (non-PQC)	400 ms	0.027 ms	2.6 ms	384 B	384 B

Іншими фіналістами в процесі NIST серед схем узгодження ключів є Crystals-Kyber на основі структурованої решітки, NTRU та SABER. Іншими альтернативними кандидатами є методи BIKE та HQC на основі кодів, NTRU Prime на основі структурованої решітки та

схема SIKE на основі ізогеній. Як видно з табл. 1, SIKE має відносно невеликі відкриті ключі та зашифровані тексти (приблизно 400 байт, і їх можна стиснути приблизно до 200 байт), але час роботи на порядки повільніший, ніж у багатьох інших кандидатів.

3.2. Схеми підписів

Кандидатами-фіналістами для схем підписів у 3-му раунді процесу NIST є схеми на базі решітки Crystals-Dilithium і Falcon і багатовимірна схема Rainbow.

Безпека Crystals-Dilithium базується на задачах решітки module-LWE та module-SIS, які є структурованими варіантами задач LWE та SIS (Short Integer Solution (коротке ціле рішення)) відповідно. Загалом Dilithium має хорошу продуктивність, помірні розміри ключа та підпису, і його легше реалізувати, ніж Falcon згідно з NIST [18].

Безпека Falcon базується на проблемі SIS, створеній за допомогою так званих решіток NTRU, які також мають додаткову структуру. Однією з цілей розробки Falcon є компактність, тобто мінімізація суми розмірів відкритого ключа та підпису. Підписання та перевірка за допомогою Falcon також ефективні, але генерація ключів повільніша порівняно з Dilithium. Як видно з табл. 2 Dilithium має найменший рекомендований набір параметрів у цій заявці – на рівні 2.

Через нові атаки на багатовимірні методи в 3-му раунді процесу NIST наразі видно, що Rainbow не буде стандартизовано [19]. Крім того, NIST планує прийняти нові пропозиції щодо схем підпису протягом 6 – 12 місяців після завершення 3-го раунду процесу стандартизації. У цьому випадку особливо будуть розглядатися ті схеми, які не базуються на структурованих решітках, див. також [20].

Таблиця 2

Середні значення продуктивності на одноядерному Intel Xeon E-2124 3,3 ГГц для деяких кандидатів на алгоритм підпису NIST PQC (і деяких поточних альтернатив, не пов'язаних з PQC) на рівні безпеки 1 NIST PQC

Алгоритм підпису	Генерація ключа	Підпис	Верифікація	Розмір відкритого ключа	Розмір підпису
Falcon (falcon512dyn)	5.9 ms	0.23 ms	0.029 ms	897 B	666 B
Dilithium (dilithium2aes)	0.015 ms	0.041 ms	0.019 ms	1312 B	2420 B
Rainbow (rainbow1aclassic363232)	2.7 ms	0.017 ms	0.0087 ms	161600 B	64 B
SPHINCS+ (SPHINCS+- SHA-256-128s-simple)	27 ms	210 ms	0.28 ms	32 B	7856 B
LMS (using SHA-256, limited to 220 messages)	-	-	-	56 B	2828 B
Ed25519 (non-PQC)	0.014 ms	0.015 ms	0.050 ms	32 B	64 B
ECDSA (P-256) (non-PQC)	0.029 ms	0.041 ms	0.086 ms	64 B	64 B
RSA-3072 (non-PQC)	400 ms	2.6 ms	0.027 ms	384 B	384 B

Серед кандидатів у процесі NIST Sphincs+ [21] є консервативним вибором як метод на основі гешу без стану. NIST розглядав Sphincs+ на 3-му раунді конкурсу як безпосередньо доступну альтернативу, якщо криптоаналітичні досягнення обмежать впевненість у безпеці фіналістів. Інші альтернативні кандидати включають Picnic і GeMSS, де Picnic базується на симетричних примітивах і техніках з нульовим знанням, а GeMSS є багатовимірною схемою підпису.

І як було сказано вище, після трьох раундів оцінки та аналізу, NIST вибрав перші алгоритми, які він стандартизує в результаті процесу стандартизації PQC і серед цифрових підписів це будуть – Crystals-Dilithium, Falcon, та Sphincs+.

4. Подальший розвиток криптографічних протоколів, оцінки та рекомендації

Французький ANSSI вже прокоментував використання QKD у документі з позицією [22]. У ньому згадуються обмеження, які вже обговорювалися тут. Серед іншого, проблематичними вважаються складне та дорогоцінне придбання, велика кількість продемонстрованих атак бічними каналами на пристрої QKD, обмежений радіус дії та відсутність наскрізної безпеки на великих відстанях. ANSSI робить висновок, що постквантова криптографія надає

альтернативу, яка є простішою та дешевшою у реалізації та не підлягає багатьом обмеженням QKD. Тому слід зосередитися на просуванні постквантової криптографії як квантово-безпечної криптографії.

NSA також вказує на технічні обмеження QKD. До них належать необхідність розповсюдження ключів для автентифікації, дороге придбання спеціалізованого обладнання та висока вразливість до атак на фізичну реалізацію та атак типу «відмова в обслуговуванні». З цих причин NSA виступає проти використання QKD у системах національної безпеки, доки не будуть усунені вищезазначені обмеження.

NCSC Великобританії також виступає проти використання QKD в урядових і військових програмах [23].

Як обговорювалося раніше, QKD має багато практичних обмежень. Деякі з них можуть бути подолані в майбутньому. Особливо бажаною була б розробка квантових повторювачів для підтримки наскрізної безпеки. Однак цього не варто очікувати найближчими роками. Крім того, європейські продукти QKD наразі недоступні на ринку. Навіть, якщо європейські продукти розробляються, їх спочатку потрібно оцінити за критеріями, які ще належить розробити. Це правда, що BSI робить перші кроки в цьому напрямку з розробкою профілю захисту. Однак поки що цей профіль захисту обмежений протоколами підготовки та вимірювання та з'єднаннями «точка-точка» та вимагає подальшого створення обширної супровідної документації.

Беручи до уваги робочу гіпотезу про те, що криптографічно відповідний квантовий комп'ютер буде доступний на початку 2030-х років, BSI вважає, що вже зараз необхідно терміново вжити відповідних заходів для переходу на квантово-безпечні схеми. Сама по собі ця нагальність робить перехід до постквантової криптографії, стандартизація якої вже добре просунута в процесі NIST, явним пріоритетом з точки зору BSI. Крім того, постквантові алгоритми набагато гнучкіші, оскільки їх можна реалізувати в існуючій інфраструктурі, вони економічніші, не вимагають секретних попередньо розподілених ключів і пропонують наскрізну безпеку.

На відміну від класичних і постквантових схем, QKD обіцяє інформаційно-теоретичну безпеку. Однак для цього потрібні відповідні докази безпеки для практично використовуваних протоколів і найзагальнішої моделі атаки. З точки зору BSI, теоретичні основи QKD ще не були задовільно розроблені в цьому відношенні. З огляду на це та сприйнятливість реалізацій до атак із стороннього каналу, «надзахищені» оцінки QKD, які іноді робляться, здаються недоречними.

Отже, з точки зору BSI, до того як QKD можна буде рекомендувати як критично важливу для безпеки технологію для практичних застосувань, ще потрібно роз'яснити багато питань і вирішити обмеження. Однак QKD і постквантова криптографія мають потенціал доповнювати одна одну, особливо тому, що вони базуються на різних принципах. Використання QKD в даний час можливо в основному в контексті експериментів для випадків обмеженого використання, де практичні обмеження менш значні, в гібридному режимі як доповнення в поєднанні з класичними і постквантовими методами узгодження ключів. Крім того, це також може забезпечити наскрізну безпеку на великих відстанях. Подальші дослідження квантової комунікації вітаються також тому, що можуть бути багатообіцяючі програми поза криптографією.

Співтовариство з безпеки та відповідні учасники чекають на завершення стандартизації NIST PQC. Наприклад, NSA все ще рекомендує набір неквантово-стійких алгоритмів відкритого ключа для захисту «цілком-секретних» [24]. Як правило, такий матеріал потребує захисту протягом десятиліть. Те, що галузь може зробити сьогодні, – це забезпечити, щоб продукти були достатньо підготовлені для переходу на алгоритми з відкритим ключем із властивостями (розміри ключа та підпису/зашифрованого тексту), подібними до пропозицій 3-го раунду стандартизації NIST PQC, коли прийде час. Схеми в стандартизації NIST PQC призначені для заміни функціональних інтерфейсів для поточного встановлення відкритого ключа та

алгоритмів підпису. Це означає, що такі протоколи, як IKEv2 і TLS, можуть продовжувати працювати, як і сьогодні, з дещо іншими характеристиками продуктивності в асиметричній частині протоколів (з відкритим ключем), коли протоколи та сертифікати оновлено для підтримки нових алгоритмів. Комунікаційні накладні витрати PQC також можуть сприяти заповненню вікон перевантаження в таких протоколах, як TCP [25].

Важко сказати, що саме станеться, коли стандартизація NIST PQC закінчиться в найближчі кілька років. Ймовірним сценарієм є те, що інші організації, які розробляють стандарти, підуть за цим і, що важливі протоколи, такі як TLS і IKEv2, будуть оновлені для підтримки нових стандартизованих алгоритмів PQC. Цілком імовірно також, що нові алгоритми мають хорошу підтримку бібліотек у важливих бібліотеках програмного забезпечення, таких як OpenSSL, на той час, оскільки робота над реалізаціями продуктивного рівня (наприклад, ефективного та безпечного від атак із синхронізованим боковим каналом) уже триває. На відміну від цього, дещо більш невизначеним є те, наскільки швидко буде розгортання в додатках, підтримка апаратного забезпечення та підтримка PKI. Ці речі мають певну ціну (наприклад, накладні витрати, проблеми із застарілою взаємодією та витрати на розгортання/розробку) для відповідних учасників, і одним із важливих факторів тут може бути реальний прогрес, досягнутий у напрямку створення великомасштабних квантових комп'ютерів у наступні декілька років. Як грубу аналогію можна розглянути, наскільки повільно додатки та суб'єкти історично поступово відмовлялися від алгоритмів (наприклад, MD5, RC4, SHA-1), безпека яких поступово, але публічно погіршувалася через криптоаналіз [26]. Однак слід враховувати не лише вартість оновлення криптографічних алгоритмів і ризики безпеки від використання погіршених алгоритмів, а й чисту вартість репутації використання погіршених алгоритмів. Подія, яка може сприяти прийняттю PQC після завершення стандартизації PQC NIST, полягає в тому, що SDO та інші важливі суб'єкти, такі як NSA, не лише оновлять стандарти та вказівки для підтримки нових алгоритмів PQC, але й припинять використання алгоритмів відкритих ключів, які зараз використовуються.

Для майбутнього використання постквантової криптографії недостатньо стандартизувати криптографічні алгоритми. Швидше, необхідно також адаптувати криптографічні протоколи до нових алгоритмів. Це пов'язано, наприклад, з тим, що в багатьох протоколах дозволена довжина відкритих ключів обмежена і більше не достатня для нових алгоритмів. Однак суттевим моментом є те, що постквантові алгоритми, як правило, не слід використовувати окремо, а лише в гібридному режимі, тобто в поєднанні з класичною процедурою. Зміни в протоколах і стандартах повинні бути ініційовані та спільно розроблені галуззю. Ця робота вже триває для багатьох протоколів.

В останні роки були запущені великі міжнародні програми з просування квантових технологій. Наприклад, Федеральне міністерство освіти та досліджень (BMBF) оголосило про свій намір сприяти розробці довгострокової безпечної криптографії та її ефективному застосуванню в додатках у рамках науково-дослідницької програми федерального уряду з IT-безпеки «Самовизначення і безпека у цифровому світі 2015 – 2020» [27]. З цією метою в серпні 2018 року було опубліковано рекомендації щодо фінансування дослідницьких проєктів на тему «постквантової криптографії». У рамках цього плану протягом 2019 – 2022 років фінансується сім проєктів для інтеграції постквантової криптографії в програми (Aquorypt), інфраструктури відкритих ключів (FLOQI), криптобібліотека Botan (KBLS), обробка медичних даних (PQC4MED), вбудовані системи (QuantumRISC), мережі (QuaSiModO) та критичні інфраструктури (SIKRIN-KRYPTOV). Загальний обсяг усіх цих проектів становить 24,2 млн. євро, при цьому частка фінансування BMBF становить приблизно 16,1 млн. євро.

Під керівництвом BMBF дослідницька програма федерального уряду «Квантові технології – від фундаментальних досліджень до ринку» [11] забезпечить федеральне фінансування у розмірі 650 млн. євро на розвиток квантових технологій у Німеччині в період з 2018 по 2022 рік.

Стимулюючий і майбутній пакет федерального уряду передбачає загалом 2 млрд. євро на розвиток квантових технологій і, зокрема, квантових обчислень, з яких приблизно 1,1 млрд. євро виділено BMBF і приблизно 900 млн. євро Федеральному міністерству економіки та енергетики (BMWi).

Зокрема, у зв'язку з просуванням квантових обчислень консультативний комітет, призначений у жовтні 2020 року, склав «Roadmap Quantencomputing» від імені Федерального уряду [28]. Мотивуючись цим, BMBF ініціював конкретні заходи фінансування для «Демонстраційних збірок квантових комп'ютерів» та «Мережі прикладних програм для квантових обчислень» у рамках фінансування поточної програми «Квантові технології – від фундаментальних досліджень до ринку». Більшість фінансування, яким керує BMWi, зосереджено на Німецькому аерокосмічному центрі (DLR) з метою розробки німецького квантового комп'ютера та відповідного програмного забезпечення та додатків.

Ще однією важливою програмою є флагманська програма ЄС з квантових технологій, що розпочалася 1 жовтня 2018 року із загалом 24 дослідницькими проєктами. Програма розрахована на 10 років і має загальний обсяг 1 млрд євро. На першому етапі з жовтня 2018 року по вересень 2021 року вона мала забезпечити загальну суму 152 млн. євро для 24 проєктів.

Проєкти охоплюють аспекти «Фундаментальна наука», «Квантові симуляції», «Квантові датчики та метрологія», «Квантові комунікації» та «Квантові обчислення». Ці та їхні плани описані в «Програмі стратегічних досліджень» [29, 30]. Зокрема, програма з квантових обчислень містить два проєкти побудови європейського квантового комп'ютера. Цей проєкт OpenSuperQ зосереджений на надпровідних кубітах, подібних до IBM, Google і Rigetti Computing та проєкту AQTION, що використовує захоплені іони і метою якого є реалізація портативного та в принципі комерційного обладнання для квантових комп'ютерів на рівні понад 50 кубітів.

У той же час Європейське спільне підприємство високопродуктивних обчислень (EuroHPC JU) переслідує цілі створення європейської інфраструктури квантового комп'ютера та сприяння дослідженням та інноваціям у цій галузі. Після переорієнтації програми у вересні 2020 року бюджет на період 2021 – 2033 років тепер становить 8 млрд. євро і включає розробку інфраструктури квантових обчислень та квантового моделювання для інтеграції в інфраструктуру високопродуктивних обчислень (HPC). Є намір побудувати такий сучасний проєкт до 2023 року.

QuNET (див. також [31]) – це національний дослідницький проєкт квантового розподілу ключів з використанням різних технологій з обсягом проекту 165 млн. євро до 2026 року, з яких BMBF виділяє 125 млн. євро для фінансування. Основними інститутами, які беруть участь у QuNET, є Інститут прикладної оптики та точного машинобудування Фраунгофера (IOF), Інститут імені Фраунгофера Генріха Герца (HHI), Інститут зв'язку та навігації Німецького аерокосмічного центру (DLR-IKN) та Інститут Макса Планка для науки про світло (MPL). У рамках проєкту будуть розроблені концепції загальної мережі та необхідної архітектури системи, а також нові ключові технології для квантового зв'язку. Також будуть враховані вимоги до стандартизації та сертифікації загальних систем QKD. Частиною підпроєкту QuNET-alpha було встановлення зашифрованого з'єднання між BMBF і BSI у Бонні в серпні 2021 року. Його було розроблено як гібридну схему шляхом поєднання постквантової схеми та QKD для узгодження ключів.

З огляду на кількість відкритих проєктів та явну зацікавленість ЄС у квантових технологіях, можна зробити висновки, що квантові технології все ще знаходяться в зародковому стані, але вже беззаперечно, що вони мають величезний економічний потенціал і значною мірою впливатимуть на інформаційну безпеку. Технологія квантових сенсорів, квантовий зв'язок і квантові комп'ютери все більше стають центром успішного довгострокового економічного розвитку Німеччини та Європи.

Висновки

1. Криптографія з відкритим ключем, що використовується в даний час, така як RSA, Діффі – Геллман, Ель Гамаль або ECC, знаходиться під загрозою квантових обчислень. Сучасні криптографічно-релевантні квантові алгоритми по суті вимагають успішної квантової корекції помилок (QEC). Криптоаналітичні досягнення на основі вже наявних пристроїв Noisy Intermediate Scale Quantum (NISQ) не можуть бути виключені. Комерціалізація квантових обчислень уже почалася, наприклад, завдяки широкому поширенню Quantum as a Service (QaaS).

2. На даний момент постквантовим криптографічним схемам, як правило, ще не довіряють такою ж мірою, як усталеним криптосистемам, оскільки вони не були добре вивчені, наприклад, з точки зору стійкості до атак бічними каналами і безпеки реалізації. Водночас, однак, необхідно своєчасно переходити на квантово-безпечні схеми. З цієї причини ідея не використовувати постквантову криптографію окремо, а лише в поєднанні з усталеними алгоритмами, загалом отримала визнання.

3. Наразі немає однозначної відповіді та дуже незрозуміло, коли і навіть, якщо CRQC коли-небудь буде побудовано. Розрив між сучасними квантовими комп'ютерами та передбачуваними CRQC величезний, і галузь стикається з деякими найближчими проблемами, такими як, наприклад, відсутність відомих програм для квантових комп'ютерів Noisy Intermediate-Scale (NISQ), які, як очікується, будуть створені найближчими роками. Найкраща поточна оцінка, яка є на даний час, полягає в тому, що комітет експертів у 2019 році дійшов висновку, що поява CRQC протягом наступного десятиліття буде дуже несподіваною.

4. Однак ризик створення CRQC означає, що наразі розгорнуту криптографію з відкритим ключем необхідно замінити квантово-стійкими альтернативами. Наприклад, інформація, зашифрована за допомогою сучасної криптографії з відкритим ключем, може бути записана криптоаналітиками, а потім піддана атаці, якщо можна створити QRQC. Потенційна шкода, яку може завдати CRQC, є основою мотивації шукати контрзаходи, навіть, якщо у нас є невизначеність щодо того, коли та чи можна створити ці комп'ютери. Оновлення розгорнутих систем, які використовують криптографію з відкритим ключем, також може тривати багато років.

5. На безпеку симетричної криптографії (включаючи криптографічні геш-функції) CRQC (включаючи розміри ключів) практично не впливають. У той час як очікується, що алгоритм Шора зможе зламати сучасну криптографію з відкритим ключем за лічені години на одному CRQC, очікується, що алгоритм, який застосовується до симетричної криптографії, алгоритм Гровера, матиме гіпотетичний час роботи багато мільярдів років на аналогічному розмірі CRQC.

6. Стандарти, наприклад, щодо протоколів, і сертифіковані продукти все ще відсутні. QKD слід використовувати лише в гібридному режимі з класичними та постквантовими схемами узгодження ключів.

7. Наскільки добре можна атакувати криптографічні алгоритми за допомогою квантових комп'ютерів, залежить не лише від прогресу, досягнутого в створенні квантових комп'ютерів, але й значною мірою від алгоритмічних інновацій. Наприклад, чи існують криптографічно відповідні квантові алгоритми, які вимагають менше кубітів? Або що обійдеться з меншим чи без квантового виправлення помилок? Або мають меншу глибину контуру? Чи можна прискорити криптографічні атаки за допомогою квантових комп'ютерів спеціального призначення? Ці запитання показують, що важливо поєднувати дослідження квантових комп'ютерів і квантових алгоритмів.

8. Також досі залишається багато відкритих питань щодо постквантової криптографії. З одного боку, стійкість до атак бічними каналами і безпека впровадження цих криптосистем ще недостатньо досліджені. З іншого боку, необхідні подальші дослідження можливих криптоаналітичних досягнень, як з класичними, так і з квантовими комп'ютерами. Зокрема, питання про те, чи структуровані та неструктуровані решітки забезпечують однакову безпе-

ку, є важливим дослідницьким питанням, яке слід шукати. З огляду на ці питання у Європейському Союзі було створено багато проєктів та ініціатив щодо дослідження багатьох питань, що стосуються постквантової криптографії та зокрема побудови великомасштабного квантового комп'ютера.

Список літератури:

1. John Preuß Mattsson, Ben Smeets and Erik Thormarker Quantum-Resistant Cryptography. Ericsson Security Research. Режим доступу: https://arxiv.org/ftp/arxiv/papers/2112/2112.00399.pdf.

2. Diane Peters. The quest to build a reliable quantum computer, 14 October 2020. [Електронний ресурс]. Режим доступу: https://www.universityaffairs.ca/features/feature-article/the-quest-to-build-a-reliable-quantum-computer/.

3. The GSMA Internet Group Quantum Computing, Networking and Security, Version 1.0, March 2021. Режим доступу: https://www.gsma.com/newsroom/wp-content/uploads/IG-11-Quantum-Computing-Networking-and-Security.pdf.

4. National Academies of Sciences, Engineering, and Medicine; Division on Engineering and Physical Sciences; Computer Science and Telecommunications Board; Intelligence Community Studies Board; Committee on Technical Assessment of the Feasibility and Implications of Quantum Computing; Emily Grumbling and Mark Horowitz: "Quantum Computing Progress and Prospects", 2019. [Електронний ресурс]. Режим доступу: https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects#toc.

5. Post-Quantum Cryptography PQC. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals.

6. M. Mosca Cybersecurity in an era with quantum computers: will we be ready? (2015). Режим доступу: https://eprint.iacr.org/2015/1075.pdf.

7. Federal Office for Information Security Quantum-safe cryptography – fundamentals, current developments and recommendations, 2022.05.18. [Електронний ресурс]. Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4.

8. Internationale Fernmeldeunion ITU-T Recommendation X.509 10/2019, October 2019. [Електронний ресурс]. Режим доступу: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

9. Deutscher Bundestag Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Anna Christmann, Kai Gehring, Margit Stumpp, weiterer Abgeordneter und der Fraktion BÜNDNIS 90 / DIE GRÜNEN – Drucksache 19/24762. Режим доступу: https://dserver.bundestag.de/btd/19/252/1925208.pdf.

10. Deutscher Bundestag Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Dr. Irene Mihalic, weiterer Abgeordneter und der Fraktion BÜNDNIS 90 / DIE GRÜNEN – Drucksache 19/25549. Режим доступу: https://dserver.bundestag.de/btd/19/263/1926340.pdf.

11. Federal Ministry of Education and Research Quantum technologies – from basic research to market, A Federal Government Framework Programme, September 2018. Режим доступу: https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Federal-Government-Framework-Programme-Quantum-technologies-2018-bf-C1.pdf.

12. Federal Office for Information Security BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths. [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/EN/Service-Navi/Publications/TechnicalGuidelines/tr02102/BSITR02102.html.

13. M. Naehrig, E. Alkim, et al. FrodoKEM, National Institute of Standards and Technology, 2020. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

14. M. R. Albrecht, D. J. Bernstein, et al. Classic McEliece, National Institute of Standards and Technology, 2020. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

15. H. Hagemeier: Frodo is the "New Hope", BSI-Magazine 2020/01, S. 12-14. [Електронний ресурс]. Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2020-01.pdf?__blob=publicationFile&v=1.

16. H. Niederreiter Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory, 15(2), S. 159-166, 1986.

17. R. J. McEliece A public-key cryptosystem based on algebraic coding theory // Technical report, NASA, 1978. Режим доступу: https://tmo.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

18. D. Moody, G. Alagic, et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, 2020, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.

19. W. Buellens Breaking Rainbow Takes a Weekend on a Laptop, February 2022. Режим доступу: https://eprint.iacr.org/2022/214.

20. National Institute of Standards and Technology NIST Status Update on the 3rd Round, July 2020. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/Presentations/2021/status-update-on-the-3rd-round.

21. A. Hülsing, D. J. Bernstein, et al. SPHINCS+, National Institute of Standards and Technology, 2020. [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

22. Agence nationale de la sécurité des systèmes d'information (ANSSI) Should Quantum Key Distribution be Used for Secure Communications?, Technical Position Paper, May 2020. Режим доступу: https://www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf.

23. National Cyber Security Center Quantum security technologies, Whitepaper, 24. March 2020. Режим доступу: https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf.

24. NSA/CSS Commercial National Security Algorithm Suite. [Електронний ресурс]. – Режим доступу: https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm.

25. Bas Westerbaan Sizing Up Post-Quantum Signatures for the Web, 31 October, 2021. [Електронний ресурс]. Режим доступу: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/anE3sBUWZS0.

26. Daniel J. Bernstein Boring crypto, University of Illinois at Chicago & Technische Universiteit Eindhoven. Режим доступу: http://cr.yp.to/talks/2015.10.05/slides-djb-20151005-a4.pdf.

27. Federal Ministry of Education and Research Self-determined and secure in the digital world 2015-2020, The German Government's research framework programme on IT security, March 2015. [Електронний ресурс]. Режим доступу: https://www.forschung-it-sicherheit-kommunikationssysteme.de/service/publikationen/self-determined-and-secure-in-the-digital-world-2015-2020.

28. VDI Technologiezentrum GmbH Roadmap Quantencomputing, October 2020. [Електронний ресурс]. Режим доступу: https://www.quantentechnologien.de/fileadmin/public/Redaktion/Dokumente/PDF/Publikationen/Roadmap-Quantencomputing-bf-C1.pdf.

29. EU Quantum Technologies Flagship Strategic Research Agenda, March 2020. [Електронний ресурс]. Режим доступу: https://qt.eu/about-quantum-flagship/resources/.

30. European Commission New Strategic Research Agenda on Quantum Technologies, February 2020. [Електронний ресурс]. Режим доступу: https://digital-strategy.ec.europa.eu/en/news/new-strategic-research-agenda-quantum-technologies.

31. Deutscher Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/17500 – Hochsicheres Quantennetzwerk QuNET. Режим доступу: https://dserver.bundestag.de/btd/19/183/1918355.pdf.

Надійшла до редколегії 05.09.2022

Відомості про авторів:

Острянська Єлизавета Вадимівна – аналітик з систем захисту інформації, АТ «Інститут Інформаційних технологій», Україна; e-mail: antelizza@gmail.com

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

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, АТ "Інститут Інформаційних Технологій", головний конструктор, Україна; e-mail: gorbenkoi@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449