[17]. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol.1№9 (115), 2022, pp. 93-101. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.253530.

ALGORITHM FOR APPLICATION OF BAYES' THEOREM FOR DETECTION OF THREATS IN INFORMATION SECURITY SYSTEMS

Information protection is becoming more relevant in today's world. This is due to the growth of technical progress and the transformation of the world into an information world. This became especially noticeable after the worldwide quarantine from the corona virus, humanity generally switched to information communication. Social networks and, in general, information communication through the worldwide network of Internet cyberspace have acquired further development. In connection with this, the scientific task of developing new and improving existing methods of information protection arises. One of the ways to improve information protection is the application of Bayes' theorem. The paper proposes the practical application of Bayes' theorem to increase the effectiveness of danger detection in the information protection and information security system of the State. Mathematical calculations proved the expediency of using Bayes' theorem to detect violations of confidentiality and truthfulness of information. According to the results of calculations using specific assumptions, we received posteriori evidence in favor of the fact that the spectrum of the signal is the spectrum of the signal of a means of secretly obtaining information is about 33:1, and for determining false information, the a posteriori chance that the information is not false information is 10:1, that is are good results. In this way, it was proved that the use of Bayes' theorem to determine the security of information according to the proposed algorithm is an improvement of the method of assessing information protection and allows solving the scientific task of increasing the effectiveness of information protection and information security of the State.

Keywords: algorithm, nonlinear system, stability, delay, forecasting, information technologies, false information, personal data.

Глухов Сергій Іванович, доктор технічних наук, професор, Завідувач кафедри військово-технічної підготовки факультету післядипломної освіти Військового інституту, Київський національний університет імені Тараса Шевченка, Київ, Україна.
Serhiy Gluhov, Doctor of Technical Science, professor, Head of the Department of Military and Technical Training of the Faculty of Postgraduate Education of the Military Institute, Taras Shevchenko National University of Kyiv.
E-mail: gluhov1971@ukr.net.
Orcid ID: 0000-0002-4918-3739.

Половінкін Ігор Михайлович, кандидат військових наук, снс, Директор Науково-методичного центру кадрової політики МО України.
Igor Polovinkin, Candidate of Military Sciences, Senior Researcher, Director of the Scientific and Methodological Center for Personnel Policy of the Ministry of Defense of Ukraine.
E-mail: Igor1964mo@i.ua.
Orcid ID: 0000-0003-0141-0274.

Кузьменко Максим Дмитрович, кандидат психологічних наук, Науково-методичний центр кадрової політики МО України.
Maksym Kuzmenko, Candidate of Psychological Science, Scientific and Methodological Center for Personnel Policy of the Ministry of Defense of Ukraine.
E-mail: kyzmenko.m.d@gmail.com.
Orcid ID: 0000-0001-9204-979X.

Пономаренко Віталій Валерійович, аспірант навчально-наукового інституту захисту інформації, Державний університет інформаційно - комунікаційних технологій.
Vitaly Ponomarenko, PhD student of the educational and scientific institute of information protection, State University of Information and Communication Technologies
E-mail: Ur_suviator@ukr.net.
Orcid ID: 0000-0002-6567-4247.

DOI: 10.18372/2410-7840.26.18835
УДК 004.056.5

МАТЕМАТИЧНІ ОСНОВИ АЛГЕБРАЇЧНИХ РЕШІТОК ТА ЇХ ЗАСТОСУВАННЯ В КВАНТОВІЙ КРИПТОЛОГІЇ

Андрій Кожухівський, Олександр Хіміч, Олександр Потій, Юрій Горбенко, Ольга Кожухівська, Юрій Борсуковський

Постійний розвиток квантових комп'ютерів загрожує найсучаснішим криптографічним схемам з відкритим ключем, таким як схеми генерації ключів на основі факторизації дискретних логарифмів, цифрових підписів та криптографії на еліптичних кривих. Необхідно розробляти нові криптографічні алгоритми, здатні протистояти атакам квантових комп'ютерів. Постквантова криптографія (PQC) спрямована на розробку алгоритмів, які можна використовувати без значних модифікацій існуючих мереж. Національний інститут стандартів і технологій США (NIST) організовує конкурс для відбору і стандартизації нових алгоритмів. Ця стаття містить огляд та аналіз процесу оцінки та відбору алгоритмів NIST на основі

задач теорії решіток. У ній даються базові визначення, описуються основні проблеми алгебраїчної теорії решіток, а також узагальнюються переваги цього класу криптографії, включаючи її стійкість до квантових обчислень. Робота робить внесок у вивчення та порівняння пост-квантових криптографічних алгоритмів, а також надає рекомендації щодо їх подальшого використання та стандартизації для забезпечення їх безпеки при розробці квантових комп'ютерів.

Ключові слова: *постквантова криптографія, алгебраїчні решітки, квантові комп'ютери, криптографічні алгоритми, теорія решіток, стандартизація криптографії.*

ВСТУП

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, що засновані на факторизації дискретних логарифмів і криптографії на еліптичних кривих, найбільш сильно постраждають. Симетричні криптографічні примітиви, такі як блокові шифри і геш-функції, будуть порушені незначно. Внаслідок цього було активізовано дослідження щодо пошуку криптосистем на відкритих ключах, які були б захищені від криптоаналітиків як з квантовими, так і з класичними комп'ютерами. Цю область часто називають постквантовою криптографією (PQC), або іноді квантово-стійкою криптографією. Її мета полягає в розробці схем, які можна розгорнути в існуючих комунікаційних мережах та протоколах без суттєвих змін.

Національний інститут стандартів і технологій знаходиться в процесі вибору одного або декількох криптографічних алгоритмів з відкритим ключем за допомогою відкритого конкурсу. Нові стандарти криптографії з відкритим ключем визначатимуть один або кілька додаткових цифрових підписів, шифрування з відкритим ключем і алгоритми встановлення ключів. Передбачається, що ці алгоритми будуть здатні добре захищати конфіденційну інформацію в недалекому майбутньому, в тому числі після появи квантових комп'ютерів.

Після багаторічного огляду кандидатів NIST вибрав 26 алгоритмів для переходу до 2-го раунду оцінки у січні 2019 року [1]. Ці алгоритми розглядалися як найбільш перспективні кандидати для можливої стандартизації і були обрані на основі як внутрішнього аналізу, так і відгуків спільноти. Під час 2-го раунду ці кандидати були піддані більш детальному аналізу з боку NIST і більш широкого криптографічного співтовариства. Після ретельного обговорення NIST вибрав сім фіналістів та вісім альтернативних варіантів, щоб перейти до 3-го раундув липні 2020 року [2]. Намір NIST полягав у стандартизації невеликої кількості фіналістів наприкінці 3-го раунду, а також невеликої кількості альтернативних кандидатів після 4-го раунду. 3-й раунд розпочався в липні 2020 року і тривав приблизно 18 місяців. Під час 3-го раунду відбувся більш ретельний аналіз теоретичних та емпіричних доказів, що використовуються для обґрунтування безпеки кандидатів. Також проводилось ретельне оцінювання їх продуктивності, використовуючи оптимізовані реалізації на різних програмних та апаратних платформах. Після трьох раундів оцінки та аналізу NIST вибрав перші алгоритми, які він стандартизує в результаті процесу стандартизації PQC.

Метою цієї статті є огляд та аналіз стану оцінювання та відбору алгоритмів в процесі стандартизації постквантової криптографії NIST, заснованої на задачах теорії решіток. Робота містить необхідні базові визначення, опис основних задач теорії алгебраїчних решіток, а також представлені основні переваги цього класу криптографії – властивість криптостійкості по відношенню до квантових обчислювачів. Вперше сутність криптоперетворення на алгебраїчних решітках у 1996 році запропонував M. Aitai [9].

ОСНОВНА ЧАСТИНА

Критерії оцінювання та процес відбору кандидатів

NIST обрав 15 алгоритмів-кандидатів для 3-го раунду. Сім з п'ятнадцяти алгоритмів були обрані у якості алгоритмів-фіналістів, в той час як інші вісім були позначені як «альтернативні варіанти» [3]. Набір фіналістів включав алгоритми, які NIST вважав найбільш перспективними, такими, що відповідають більшості випадків використання, і найімовірніше, що будуть готові до стандартизації незабаром після закінчення 3-го раунду. Альтернативні кандидати вважалися потенційними кандидатами для майбутньої стандартизації, швидше за все, після чергового раунду оцінки. Деякі з альтернативних кандидатів мають гірші характеристики ефективності, ніж фіналісти, але можуть бути вибрані для стандартизації на основі високої впевненості NIST у їх безпеці. Інші мають прийнятну ефективність, але потребують додаткового аналізу чи іншої роботи, щоб забезпечити достатню гарантію їх безпеки для

стандартизації NIST. Крім того, деякі альтернативні кандидати були обрані на основі прагнення NIST до різноманітності в майбутніх постквантових стандартах безпеки або на їх потенціалі для подальшого вдосконалення. Сім фіналістів включали у себе чотири механізми інкапсуляції ключів (KEM) та три механізми цифрового підпису. З восьми альтернативних варіантів п'ять – KEM та трицифрові підписи. Командам подання було дозволено внести незначні модифікації та повторно подати свої пакети, які повинні були відповідати тим же вимогам, що і оригінальні подання. Повні оновлені технічні характеристики були розміщені на веб-сайті PQC NIST [4] 23 жовтня 2020 року для публічного огляду.

У Call for Proposals NIST [5] визначено три широкі аспекти критеріїв оцінки, які будуть використовуватися для порівняння відповідних алгоритмів в процесі стандартизації PQC NIST: 1) безпека, 2) вартість і продуктивність, 3) характеристики алгоритму і реалізації. Ці критерії описані разом з обговоренням того, як вони вплинули на оцінювання кандидатів у 2-му раунді. Наведені вище аспекти критеріїв оцінки детально розглянуті в [6].

Як і у випадку з минулими конкурсами Розширений стандарт шифрування (AES) і Безпечний алгоритм гешування (SHA-3) є найбільш важливим фактором, що NIST використовує при оцінці кандидатів на постквантові алгоритми. Нинішні стандарти з відкритим ключем NIST використовуються у самих різних додатках, включаючи Інтернет-протоколи, такі як TLS, SSH, IKE, IPsec і DNSSEC, а також для сертифікатів, підпису програмного коду і безпечних завантажувачів.Нові стандарти NIST на відкритому ключі забезпечать постквантову безпеку для кожного з цих додатків. Для кількісної оцінки безпеки можливих алгоритмів NIST дав три можливі визначення безпеки – два для шифрування і одне для підпису. NIST також визначив п'ять категорій безпеки для класифікації обчислювальної складності атак, які порушують визначення безпеки [7].

NIST також згадував інші бажані властивості безпеки, такі як пряма безпечність, стійкість до атак бічними каналами та багатоключових атак, а також стійкість до неправильного використання. У деяких випадках NIST закликає представників внести незначні зміни, щоб забезпечити або вдосконалити ці додаткові бажані властивості безпеки (наприклад, додавання відкритої солі до шифртекстів, щоб уникнути багатоцільових атак на KEM).

Що стосується схем шифрування загального призначення і встановлення ключів, то у Call for Proposals [7] використовувалися «семантично безпечні» схеми щодо атаки на основі адаптивно вибраного шифртексту (що еквівалентно безпеці IND-CCA2). Для одноразових випадків використання NIST також приймав алгоритми, що забезпечують семантичну безпеку щодо атаки на основі вибраного відкритого тексту (безпека IND-CPA). IND-CCA2 – безпека не потрібна в строго одноразових випадках використання, і спроба задовольнити більш суворі вимоги IND-CCA2-безпеки може спричинити за собою значні втрати продуктивності для деяких схем. Схеми цифрового підпису повинні були забезпечити екзистенційно непідробні підписи стосовно атаки на основі адаптивно вибраного повідомлення (EUF-CMA безпека). Автори заохочувалися, але не були зобов'язані надавати докази безпеки у відповідних моделях.

П'ять категорій безпеки, які визначені у [7], були засновані на обчислювальних ресурсах, необхідних для виконання певних атак методом перебору проти існуючих стандартів NIST для AES і SHA в різних моделях вартості обчислень як класичних, так і квантових.

Числа обчислювальної продуктивності з [7] для процесора x86-64 з розширеннями R^n AVX2 для Kyber, NTRU та Saber для категорій безпеки 1 та 3, а також загальні витрати для Kyber, NTRU та Saber, коли додається вартість передачі даних, приведені в [6]. Інкапсуляція та декапсуляція є дуже швидкими з усіма трьома схемами. Незважаючи на те, що Saber має найнижчу загальну вартість завдяки меншим відкритим ключам та шифротекстам, різниця у вартості між Kyber та Saber не була достатньо великою, щоб вважатися значною.

Попередня інформація щодо моделей та визначення безпеки на основі коду та багатовимірних перетворень, що представляють деякі складні обчислювальні проблеми, які є загальними для багатьох схем на основі кодів, багатовимірних схем або схем на решітках, досліджених у процесі стандартизації NIST PQC, приведені в [6].

Розглянемо схеми на основі алгебраїчних решіток. 7 із 15 кандидатів 3-го раунду є криптосистемами на основі решітки. Ці криптосистеми пов'язані з великою кількістю академічних досліджень, які наголошують на (асимптотичній) доказовій безпеці, заснованій на найгіршому сценарії складності проблем решітки. Ранньою віхою в цьому напрямку досліджень стала стаття Ajtai

1996 р. [9], яка визначила проблему короткого цілого розв'язку (SIS) і пов'язала її середню складність із найгіршою складністю пошуку коротких векторів у кожній цілочисельній решітці, даючи односторонні функції на основі решітки та односторонні функції з секретом на основі решітки.

В [6] коротко описано різні базові проблеми безпеки для кожної з цих систем. Оцінка вартості вирішення цих критичних проблем безпеки на примірниках решітки реального світу є дуже нетривіальною, оскільки передбачає вибір найкращого типу атаки та оптимізацію параметрів атаки, щоб знайти найкраще можливе рішення із заданою кількістю обчислювальних ресурсів. Теоретичні межі та комп'ютерне моделювання використовуються для того, щоб оцінити вартість вирішення надзвичайно великих випадків цих проблем. Останніми роками це було предметом інтенсивних досліджень, які призвели до надійних оцінок конкретної безпеки криптосистем на основі решітки. Перспективними кандидатами на роль таких оцінок стали задачі теорії решіток. Задачі теорії решіток лежать в основі цілого класу криптографічних примітивів та протоколів «постквантової криптографії». Як приведено вище, до третього раунду залишилося 15 кандидатів, з них 7 кандидатів 3-го раунду є криптосистемами на основі решіток. Решітка – це дискретна підмножина векторів (точок) у евклідовому просторі R^n, яка є замкненою за операціями додавання та віднімання векторів. Решітка має розмірність n, якщо вона розміщується у будь-якому підпросторі простору R^n. При геометричному поданні решітка – це множина, що рівноймовірно розміщена у просторі R. За своїми властивостями алгебраїчна решітка є абелевою групою. Основою побудування алгебраїчної решітки L є множина векторів B, таких, що будь-яка точка (вектор) L може бути представлена у вигляді лінійної комбінації елементів B. Огляд та аналіз стану оцінювання та відбору процесу стандартизації постквантової криптографії NIST, заснованого на задачах теорії решіток, проведемо на прикладі фіналістів третього раунду Kyber, NTRU та Saber, які визначені NIST як алгоритми, що покладаються на структуровані решітки.

У свою чергу, алгебри, засновані на квантових обчислювачах [8], дозволили реалізувати алгоритми розшифрування повідомлень та пошук колізії за поліноміальний час для задач $NPco$ $NP(=P)$ класу. В результаті виникла потреба у теоретичних дослідженнях і практичній реалізації нового покоління криптографічних протоколів і примітивів, заснованих на NP-повних задачах, які дозволяють реалізовувати розв'язування таких задач швидше, ніж із субекспоненційною складністю [9].

Нині все більш актуальною стає проблема захисту інформації та ресурсів від існуючих та потенційних криптоаналітичних атак з використанням квантового комп'ютера та квантової математики. Це обумовлено розробкою математичних основ для квантового комп'ютера та безпосередньо стрімким розвитком теорії та практики квантових комп'ютерів [9,10].Розуміючи цю проблему, технологічно розвинені держави суттєві зусилля направляють на аналіз криптографічної стійкості існуючих стандартів криптографічного захисту інформації у постквантовий період та ведуть пошук щодо створення постквантових стандартів асиметричної криптографії. По суті, виникла необхідність розгляду та аналізу існуючих на сьогодні криптографічних алгоритмів, заміни їх параметрів або збільшення розміру цих параметрів, а також необхідність створення нових стандартизованих криптографічних алгоритмів з огляду на можливості квантового комп'ютера та його математичного забезпечення у постквантовий період. Вирішення цієї проблеми здійснюється на світовому рівні в процесі проведення NIST США міжнародного конкурсу [11]. NIST США, розуміючи необхідність пошуку нових стандартизованих асиметричних криптографічних примітивів, особливу увагу звертає на створення цифрового (електронного) підпису (ЕП).

Як показують попередні дослідження, надійною математичною основою, на якій можуть бути створені постквантові ЕП, нині вважаються алгебраїчні решітки [7]. По суті, такий математичний апарат пройшов випробовування часом у вигляді регіонального стандарту X9.98 [10, 11].

З огляду на вищевказане, актуальною є проблема аналізу, дослідження, оцінки та порівняння кандидатів на постквантові стандарти ЕП з використанням математики алгебраїчних решіток, а також розробки рекомендацій щодо вибору із них найбільш перспективних для майбутнього застосування.

Тому вивчення та уточнення властивостей задач теорії решіток – це одна з основних задач як при побудові, так і при криптоаналізі примітивів і протоколів на основі задач теорії решіток. Важливість цього напряму досліджень обумовлена також наявністю у задач теорії решіток (при

деяких параметрах) властивостей криптостійкості до алгоритмів, що виконуються на квантових комп'ютерах.

Основи теорії алгебрайчних решіток

Перед тим, як перейти до викладу формулювання цих задач, уведемо необхідний набір визначень [9, 14, 15]. Решітка – дискретна адитивна підгрупа, яка задана на множині R^n, тобто решітку L можна представити як безліч цілочисельних лінійно незалежних базисних векторів (рис. 1):

$$B=\{b_1,\cdots,b_n\}\subset R^n, L=\sum_{i=1}^{n} b_i\cdot Z=\{B_x: x\in Z^n\}.$$

У решітки може бути безліч базисів: $L=\sum_{i=1}^{n} a_i\cdot Z$ (рис. 2).

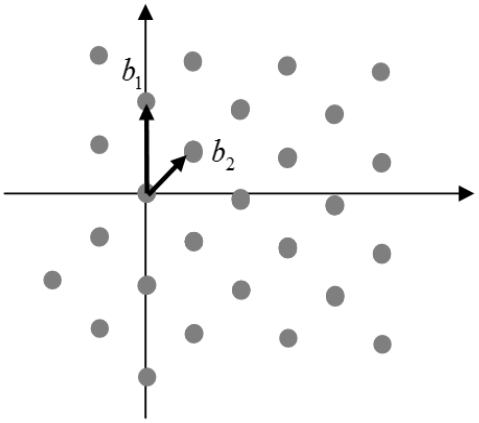

Рис.1. Решітка з базисом $\{\bar{b}_1,\bar{b}_2\}\in B$

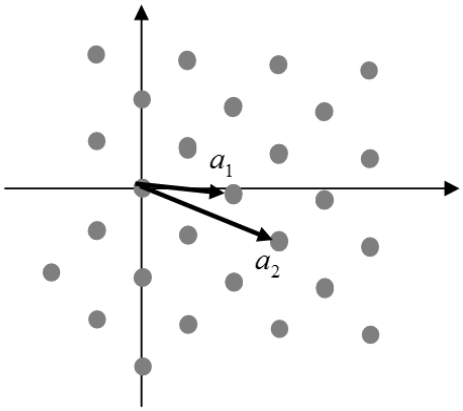

Рис.2. Решітка з базисом $\{\bar{a}_1,\bar{a}_2\}\in B$

Далі показано фундаментальні паралелепіпеди, утворені базисами. Площі (обсяги в багатовимірному випадку) фундаментальних паралелепіпедів, утворених різними базисами однієї решітки L, $\det(L)$ будуть рівними (рис. 3, 4). Тобто, $\det L$ є інваріант решітки. Під найкоротшим вектором решітки розумітимемо вектор з координатами $\lambda_1(L)=\min\limits_{x,y\in L,x\neq y}\|x-y\|=\min\limits_{x\in L,x\neq 0}\|x\|$ (рис. 5). Тоді багатовимірним узагальненням цього поняття буде $\lambda_1(L)$, обмежене мінімальним r, для якого розмірність решітки всередині кулі радіуса r більша або дорівнює k (рис. 6).

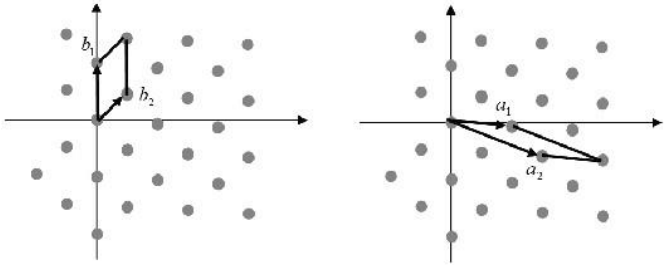

Рис. 3, 4. Фундаментальні паралелепіпеди, утворені базисами

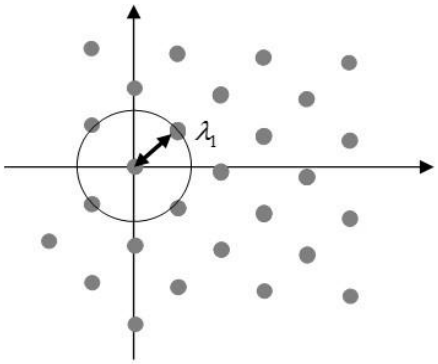

Рис. 5. Найкоротший вектор

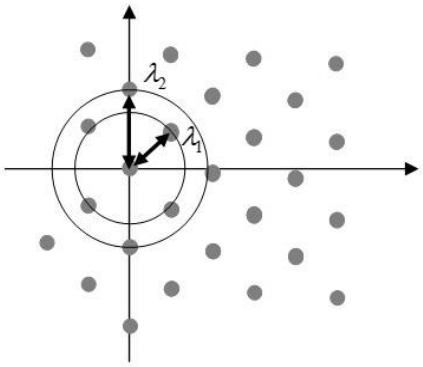

Рис. 6. Найкоротший базис решітки L в R^2

Таким чином, познайомившись з основними визначеннями теорії решіток, перерахуємо задачі, що активно застосовуються в криптографії [9, 14, 15]:

1. За базисом решітки знайти найкоротший ненульовий вектор (shortest vector problem, SVP, пошук найкоротшого вектора) (рис. 7);

2. За базисом решітки $B\in Z^{m\times n}$ і дійсним $\gamma\succ 0$ знайти ненульовий вектор $\bar{b}\in BZ^n\setminus\{0\}$: $\|\bar{b}\|_p\le\gamma\lambda_1^p(L)$ з p-нормою (γ- approximation shortest vector problem, SVP_γ^p; наближений пошук найкоротшого вектора) (рис. 8);

3. За базисом решітки B і заданим вектором $\bar{j}\notin L(B)$ знайти найближчий вектор $\bar{b}\neq L(B)$ (Clos-

es Vector Problem, CVP; пошук найближчого вектора є неоднорідним (гетерогенним) варіантом SVP-задачі) (рис. 9);

4. За базисом решітки $B \in Z^{m\times n}$, дійсним $\gamma \succ 0$ і заданим вектором $\bar{j} \in LR^n$ знайти ненульовий вектор $\bar{b} \in BZ^n : \left\|\bar{j}-\bar{b}\right\|_p \le \gamma\lambda_1^p(L)$ з p-нормою (γ – approximate closes vector problem, SVP_γ^p;

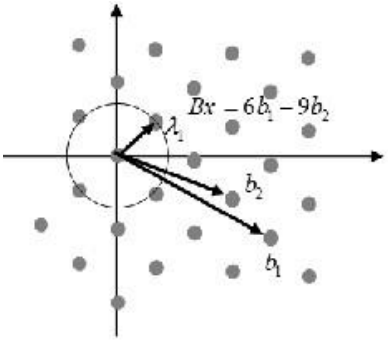

Рис. 7. Приклад SVP-задачі в R^2

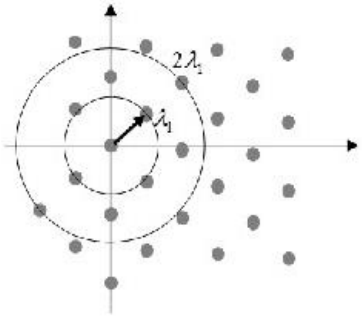

Рис. 8. Приклад SVP_γ-задачі в R^2

5. Нехай дана n-мірна решітка L. Знайти лінійно незалежні вектори $\bar{b}_1,\cdots,\bar{b}_n \in L$, для яких $\max\limits_{i=1}^{n}\left\|\bar{b}_i\right\| \le \gamma\lambda_n^p(L)$, де $\lambda_n^p(L)$ – i-й послідовний мінімум у решітці з p - нормою (γ-approximate shortest independent vector problem, $SIV_\gamma^p(n,\gamma)$; наближений пошук найкоротших лінійно незалежних векторів) (рис. 10);

6. Нехай дана n-мірна решітка L. Знайти вектор $\bar{u} \in L\setminus\{0\}: \left\|u\right\|_p \le \gamma\lambda_1^p(L)$, де $\lambda_1^p(L)$ – це довжина найкоротшого вектора в решітці з p-нормою і $\bar{u}$ - найкоротший γ - унікальний вектор, тобто, $\forall w \in L : \lambda_1^p(L) \le \left\|\bar{w}\right\|_p \le \gamma\lambda_1^p(L)$, $\bar{w} = z\bar{u}$ для деяких $z \in Z$ (γ-approximate unique shortest vector problem, $uSVP_\gamma^p(n,\gamma)$; пошук унікального найкоротшого вектора) (рис. 11);

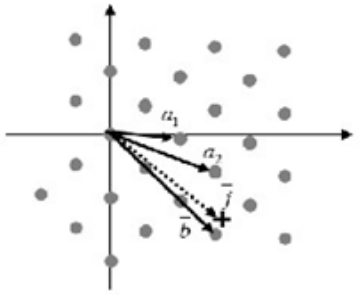

Рис. 9. Приклад CVP-задачі в R^2

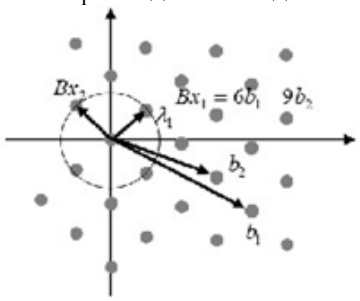

Рис. 10. Приклад $SIVP$-задачі в R^2

7. Нехай даний базис B q-нарної (модулярної) m-мірної решітки $L_q^{m\times n}$, тобто, решітки L, для якої приналежність вектора до решітки L визначається: $L(B)=\{B^T s \bmod q \subseteq Z^m, s\in Z^n\}$, q – просте число. На решітці рівномірно розподілений шум e (зазвичай з моментом очікування, рівним 0 і дисперсією $\sqrt{q}$), q заданий деяким багаточленом, $\bar{s} \in Z_q^n$ - деякий початковий вектор без шуму, відомо значення $(B\bar{s}+\bar{e})$. Знайти початкову точку в решітці (виключити шум) по деякій множині відомих $(B\bar{s}_i+\bar{e}_i)$. Задача навчання з помилками (Learning with errors, LWE) є узагальненням задачі навчання контролю цілісності (парності) даних із шумами (рис. 12);

8. Нехай дана m-мірна модулярна решітка $L_q^{\perp}(B)=\{\bar{x}\in Z^m : B\bar{x} \equiv \bar{0}\, Z^n \bmod q\}$, яка утворена базисом $B\in Z_q^{n\times m}$, взятим випадково з рівномірного розподілу над $Z_q^{n\times m}$. Знайти найкоротший вектор $\bar{v} \in L_q^{\perp}(A): \left\|\bar{v}\right\|_p \le \beta$ з p-нормою (Short integer solution problem, $SIS_\beta^p(n,m)$; задача пошуку вектора за нормою в модулярній решітці);

9. Нехай дана m-мірна модулярна решітка $L_q^{\perp}(B)=\{\bar{x}\in Z^m : B\bar{x} \equiv \bar{0}\, Z^n \bmod q\}$, яка утворена базисом $B\in Z_q^{n\times m}$, і вектор $\gamma \in Z^n$, взяті випадково з рівномірного розподілу над $Z_q^{n\times m}$, Z^n відповідно. Знайти вектор $\bar{v} \in \{\bar{x}\in Z^m : A\bar{x} \equiv \bar{y} \bmod q\}$:

$\|\bar{v}\|_p \le \beta$ (Short integer solution problem, $ISIS_\beta^p(n,m)$; гетерогенна задача пошуку вектора за нормою в модулярній решітці);

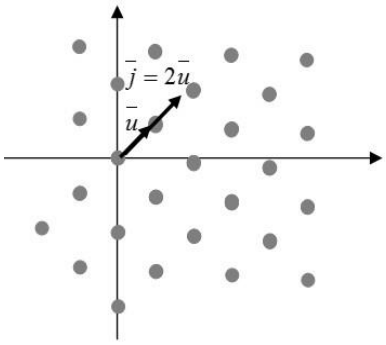

Рис. 11. Приклад $uSVP$-задачі

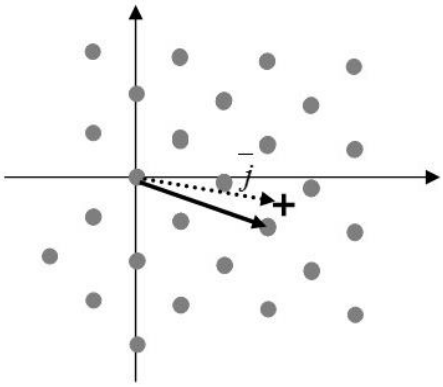

Рис. 12. Приклад BDD-задачі

10. За базисом решітки $B \in Z_q^{n\times m}$ і дійсним $\gamma \ge 1$ знайти ненульовий вектор $\bar{b} \in BZ^n \setminus \{0\}$: $\|\bar{b}\|_p \le \gamma \cdot \det(L(B))^{1/n}$ з p-нормою (γ-approximate Hermite shortest vector problem, hermit SVP_γ^p; задача наближеного пошуку найкоротшого вектора за Ермітом);

11. Нехай дана n- мірна решітка $L^n \subseteq R^k$. Знайти базис B: $\forall\ B' \in \{B \in Q^{n\times k} : L = L(B)\}$, $\max_{i=1}^{n}\{\|\bar{b}_i\|_p\} \le \gamma \max_{i=1}^{n}\{\|\bar{b}_i\|_p\}$ (γ – approximate shortest basis problem, $SVP_\gamma^p(n)$; наближений пошук найкоротшого базису);

12. Нехай n – мірна решітка L^n задана деякою p - нормою. Знайти довжину $l^{(p)} \in R$: $l^{(p)} \le \lambda_1^{(p)}(L) \le \gamma l^{(p)}$, де $\lambda_1^{(p)}(L)$ – довжина найкоротшого вектора або перший послідовний мінімум в решітці L (γ – approximate shortest length problem, $SLP_\gamma^p(n)$; задача наближеного пошуку довжини найкоротшого вектора в решітці);

13. За базисом решітки $B \in Z^{m\times n}, m \ge n$ і радіусом $r \in R$ відповісти на питання: «так» – якщо всі точки решітки можна покрити радіусом r, $r \ge p(L(B))$; «ні» – якщо $\gamma \cdot r \prec p(L(B))$ (γ – approximate covering radius problem, $SRP_\gamma^p(n,r)$; наближена задача покриття решітки радіусами);

14. За базисом решітки $B \in Z^{m\times n}$, дійсним $a \ge 1$ і вектором $\bar{u}: \exists \bar{t} \in L(B), \|\bar{u} - \bar{t}\|_p \prec a \cdot \lambda_1^p(L)$ знайти вектор $\bar{v} \in L(B): \|\bar{u} - \bar{t}\|_p = \min$ (α – approximate bounded distance decoding, $BDD_a^p(u)$; наближена задача про декодування з обмеженою відстанню);

15. За базисом $B \in Z^{m\times n}$, вектором решітки $v \in BZ^n$ і позитивним дійсним числом $d, \gamma \succ 0$ відповісти на запитання: «так» – якщо $\min\{\|v\|_p : v \in \mathrm{BZ}^n \setminus 0\} \le d$; «ні» – якщо $\min\{\|v\|_p : v \in \mathrm{BZ}^n \setminus 0\} \succ \gamma d$; (Decisional shortest vector problem, $GapSVP_\gamma^p$; Булева задача про пошук найкоротшого вектора);

16. За базисом $B \in Z^{m\times n}$, вектором решітки $t \in BZ^n$ і позитивними дійсними числами $d, \gamma \succ 0$ відповісти на запитання: «так» – якщо $\min\{\|t - v\|_p : v \in \mathrm{BZ}^n\} \le d$; «ні» – якщо $\min\{\|t - v\|_p : v \in \mathrm{BZ}^n\} \succ \gamma d$; (Decisional closest vector problem, $GapCVP_\gamma^p$; Булева задача пошуку вектора, близького до вектора у решітці);

17. Нехай дано ідеал $I \in Z(x) / f(x)$. Знайти багаточлен $g(x) \in I \setminus \{0\}$: $\|g \bmod f(x)\|_p \le \gamma \lambda_1^p(I)$ (Approximate ideal shortest vector problem/Shortest polynomial problem, $Ideal - SVP_\gamma^p(f)$; наближена задача пошуку найкоротшого вектора в ідеальній решітці: завдання пошуку найкоротшого полінома);

18. Нехай дані m – багаточленів $g_1(x), \cdots, g_m(x)$, вибраних випадково з рівномірного розподілу, заданого на $Z_q(x) / f(x)$ і n – степінь багаточлена. Знайти цілі $e_1, \cdots, e_m \in Z(x)$: $\sum_{i \le m} e_i g_i = 0 \pmod q, \|e\|_p \le \beta$, де вектор e отримується шляхом конкатенацій (об'єднанням) коефіцієнтів при всіх e_i (Ideal small integer solution problem, $Ideal - SIS_\beta^p(g,n,m)$; задача пошуку вектора за нормою в ідеальній решітці).

Оцінка вартості вирішення цих критичних проблем безпеки на примірниках решітки реального світу є дуже нетривіальною, оскільки передбачає вибір найкращого типу атаки та оптимізацію параметрів атаки, щоб знайти найкраще можливе рішення із заданою кількістю обчислювальних ресурсів. Теоретичні межі та комп'ютерне моделювання використовуються для того, щоб оцінити вартість вирішення надзвичайно великих випадків цих проблем. Останніми роками це було предметом інтенсивних досліджень, які призвели до надійних оцінок конкретної безпеки криптосистем на основі решітки.

Теорія решіток вважалася завершеною, будучи дослідженою Лагранжем, Гаусом, Діріхле та іншими видатними математиками. Незважаючи на те, що до 1996 р. оцінки складності були відсутні і єдине, що було відомо, SVP є NP-повною задачею [12].

У 1996 р. угорський математик-дослідник IBM Міклос Айтаї у своїй роботі [9] показав, що:

- можливо побудувати односторонню функцію на основі SVP-задачі; пізніші дослідники покращили результат до «односторонньої функції із секретом» (trapdoor function, [9]) – варіантом односторонньої функції, яка швидко обертається (у порівнянні зі швидкістю отримання образу функції) за наявності додаткових відомостей;

- переформульована в ймовірнісний варіант задачі про рюкзак, SVP-задача немає ймовірнісного поліноміального алгоритму рішення, тобто, не розв'язувана за поліноміальний час на квантових обчислювачах;

- серед усього класу NP-задач SVP-задача є складною, тобто, є NP-повною задачею.

Робота Айтая продемонструвала перевагу протоколів шифрування та криптографічних примітивів на основі задач теорії решіток перед традиційними системами шифрування, заснованими на геш-функціях, що містять колізії, задачах факторизації чисел (RSA) та дискретного логарифмування (ECC), що належать $NP \cap coNP$-класу.

Розглянувши задачі теорії решіток, наведемо ключову теорему Айтаю, що лежить в основі шифрування на основі задач теорії решіток [9]: визначимо для будь-якого натурального $n \in N$ клас випадкових решіток L^n, що породжуються з поліноміальною часовою складністю. Припустимо, що існує поліноміальний за часовою складністю алгоритм A такий, що для будь-якої випадково вибраної решітки $L \subset R^n$ знайде нетривіальний вектор $\bar{v}$, довжина якого не перевищує n. Отже, існує ймовірнісний поліноміальний за часовою складністю алгоритм B, який для будь-якої решітки $L \subset R^n$ і деяких констант c_0, c_1, c_2 з високою ймовірністю здатний вирішити будь-яку з наступних задач:

- SVP_γ - задачу з точністю $\gamma = n^{c_2}$;
- $SIVP_\gamma$ - задачу з точністю $\gamma = n^{c_0}$;
- SBP_γ - задачу з точністю $\gamma = n^{c_1}$.

Цією теоремою Айтай встановив зв'язок між складністю в гіршому і середньому випадках перерахованих вище задач, а так само продемонстрував механізм створення односторонніх функцій. Цай і Неруркар у 1997 р. знизили значення констант: $c_0 \succ 3, c_1 \succ 3.5, c_2 \succ 4$ [14]. Даніель Міссіансіо та Одед Реджев у 2004 р. показали, що $c_2 = 1$ [15]. Гольдштейн, Гольдвасер і Халеві, досліджуючи односторонні функції Айтаю, довели наявність у деяких класів решіток сильніших властивостей – властивостей криптографічних геш-функцій [16]. Саме наявність зв'язку між складністю в гіршому і середньому випадках дозволяє побудувати деяку систему шифрування на основі однієї із задач теорії решіток, взятої з відомого випадкового розподілу, тим самим отримавши сувору оцінку складності розшифровки цієї системи (криптостійкості) у гіршому випадку. Слід так само відзначити, що більшість криптографічних примітивів і протоколів (RSA, ECC та інші) не мають даної властивості, а засновані на складності в середньому, що значно ускладнює як вибір параметрів шифрування, так і суворий доказ складності їх розшифровки.

Кожна із задач теорії решіток, залежно від параметрів (наприклад, точності рішення), належить до деякого класу тимчасової (ємнісної) складності для детермінованої та недетермінованої машин Тьюринга [17]. При аналізі задач увага концентрується саме на часовій складності, як ключовому параметрі захищеності (власне ємнісна складність явно не перевищує часову). Задачі допускають взаємні редукції, що спрощує їх дослідження, наприклад: $SBP_\gamma^p(n) \le SIVP_\gamma^p(n)$ [18]; $uSVP_\gamma \le BDD_{1/\gamma} \le uSVP_{2/\gamma}$ [19]; $GapCVP_\gamma^p \equiv CVP_\gamma^p$, $SBP_\gamma^2 \le CVP_\gamma^2$ [20]. Покажемо на прикладі редукцію SVP^p і CVP^p-задач [21, 22].

Від CVP^p до SVP^p: Нехай дано майже ортогональний базис, що утворює n-мірну решітку $L(B): B = \{\bar{b}_1, \cdots, \bar{b}_n\}$. Визначимо решітку $L'(B'): B =$

$\{2\bar{b}_1,\cdots,\bar{b}_n\}$ і розв'яжемо CVP^p-задачу для вектора $\bar{b}_1$ і решітки $L^{'}(B^{'})$, отримавши вектор $\bar{v}\in L^{'}$. Обчислимо новий вектор $s_1=\bar{v}-\bar{b}_1$. Виконаємо попередні дії для векторів $\bar{b}_2,\cdots,\bar{b}_n$, отримавши вектори $\bar{s}_2,\cdots,\bar{s}_n$. Знайдемо найкоротший із векторів $\bar{s}_1,\cdots,\bar{s}_n$. Від SVP^p до CVP^p: Нехай дано базис, що утворює n-мірну решітку $L_0^n(B^{'}):B^{'}=\{\bar{b}_1,\cdots,\bar{b}_n\}, B\in Z^n$ та деяка точка $y\notin L^n(B^{'})$. Розв'яжемо першу частину SVP^p задачі, виконавши ортогоналізацію базису, як необхідну умову пошуку найкоротшого вектора. Обчислювати довжини векторів, а також вибирати серед них найкоротший вектор в даному випадку немає необхідності. Отримаємо решітку $L^n(B)\equiv L_0^n(B^{'})$. Знайдемо вектор $\bar{a}\in R^n$, розв'язавши лінійну систему рівнянь $B\bar{a}=y$. Округливши координати отриманого вектора до цілих значень, отримаємо шуканий вектор $\bar{z}\in Z^n$.

Складність CVP^p- задачі перевершує складність SVP^p- задачі, так як необхідним елементом розв'язання CVP-задачі є найбільш ресурсомістка частина задачі пошуку найкоротшого вектора, а саме приведення базису решітки до ортогонального вигляду. Складність обчислення довжин векторів залежатиме від норми $O(n\log n)$ (для норм Евкліда ℓ_2 [23]), а складність знаходження мінімального елемента буде $O(n)$ в гіршому випадку. Причому від якості базису буде залежати похибка CVP^p - алгоритму для запропонованого алгоритму $\varepsilon=\|B\bar{a}-B\bar{z}\|\le\frac{1}{2}\left\|\sum_i b_i\right\|$. Наприклад, для решіток $L_1(B_1)\equiv L_2(B_2),|\det(B_1)|-|\det(B_2)|$, утворених базисами $B_1=\{(1,0),(0,1)\}$, $B_2=\{(100,1),(99,1)\}$, $\varepsilon_1=1.4,\varepsilon_2\approx199$ похибка буде відповідною.

На основі задач *GapSVP* та *SIVP* Айтаєм у 1996 р. [9] були запропоновані методи реалізації вільних від колізій геш-функцій.

Розглянемо цю геш-функцію Айтая докладніше, оскільки інші алгоритми шифрування побудовані за аналогією.

Функція Айтая – це функція виду $f_a(x)=Ax \bmod q$, де $A\in Z_q^{n\times m}$ і $x\in\{0,1\}^m$. Наприклад, при $q=10$, $n=4$, $m=7$:

$$f_a(x)=Ax\,mod q=\begin{pmatrix}1&2&3&4&5&6&7\\0&5&6&8&4&3&0\\1&7&3&7&3&2&9\\4&8&2&5&2&1&4\end{pmatrix}\cdot\begin{pmatrix}0\\1\\0\\1\\1\\0\\0\end{pmatrix}mod\,10=(1\quad 7\quad 7\quad 5).$$

Параметри криптографії задаються з таких міркувань: n- основний параметр, що визначає захищеність $q=n^{o(1)}, O(n\log n)\succ n\log_2 q$; останнє обумовлено тим, що при $n\ll m$ задачу стискання легко можна розв'язати. Наприклад, n = 1024, q = 232, m = 65536. Тобто, функція Айтая $f_a(x)$ – стискає m-вихідних біт в $n\log_2 q\prec m$, в даному випадку 65536 стискає в 32768 біт. Покажемо зв'язок із теорією решіток: ядром множини $A\in Z_q^{n\times m}$ є решітка $L(A)=\{z\in Z^m: Az=0 \pmod q\}$. Тоді колізія геш-функції $(f_a(x)=f_a(y), x\ne y)$ стане вектором виду $z=(x-y)\in\{-1,0,1\}: Az=Ax-Ay=0 \bmod q$ або $z_i\in L(A)$ із нормою $\|z\|_\infty=\max_i|z_i|=1$. Тобто, пошук колізій геш-функції Айтая $f_a(x)$ відповідає розв'язку SVP-задачі в решітці L.

Колектив учених Голдштейн-Голдвассер-Халеві (GGH) [24] у 1997 р. запропонував варіант геш-функції на основі псевдокуба, побудованого на векторах деякої решітки L.

Місіансіо та Реджев [16] запропонували загальний підхід до шифрування, заснований на додаванні шумів у решітку, що дозволяє отримати решітку, яка не відрізняється від рівномірного розподілу. Потім, шляхом розбиття решітки на комірки, побудувати відображення, що дозволяє реалізувати вільну від колізій геш-функцію і протокол асиметричного шифрування. Ця концепція визначила сучасний напрямок розвитку криптографії на основі теорії решіток.

Розглянемо циклічну решітку – це решітка виду $A=[A^{(1)}|\cdots|A^{(m/n)}]$, $A^{(i)}\in Z_q^{n\times n}$, тобто, решітка, що характеризуються деякою постійною структурою, одержуваною в результаті перестановки елементів за деяким правилом, наприклад:

$$A^i=\begin{bmatrix}a_1^{(i)}&a_n^{(i)}&\cdots&a_2^{(i)}\\a_2^{(i)}&a_1^{(i)}&\cdots&a_3^{(i)}\\\vdots&\vdots&\ddots&\vdots\\a_n^{(i)}&a_{n-1}^{(i)}&\cdots&a_1^{(i)}\end{bmatrix},A^1|A^2|A^3=$$

$$\left|\begin{matrix}7&1&4&3\\3&7&1&4\\4&3&7&1\\1&4&3&7\end{matrix}\right\|\left\|\begin{matrix}0&2&3&4\\4&0&2&3\\3&4&0&2\\2&3&4&0\end{matrix}\right\|\left\|\begin{matrix}9&3&5&1\\5&9&3&5\\1&5&9&3\\3&1&5&9\end{matrix}\right|.$$

Кріс Пеінкерт та Алон Розен у 2006 р. [25] запропонували свій варіант геш-функції, заснованої на круговій загальній $SIVP$ - задачі на циклічних решітках: заданий вектор визначений цілочисленним поліномом $P(a)\neq 0 \mod (a^n-1)$, необхідно знайти множину або підмножину лінійно незалежних векторів з нормою, пропорційною величині норми загальних векторів полінома і решітки. Геш-функція Пеінкерта-Розена має важливі властивості, які виділяють її серед усіх інших функцій лінійною залежністю довжини образу геш-функції від її про-образу та лінійним зростанням складності обчислень за часом.

Одночасно зі створенням криптографічних примітивів були запропоновані такі системи асиметричного шифрування на основі решіток розмірності n:

- система Ajtai-Dwork заснована на $uSVP$ - задачі з публічним ключем довжини n^4;

- система Goldreich-Goldwasser-Halevi (GGH), заснована на наближеній CVP-задачі, з публічним ключем довжини n^2;

- система NTRU (Draft standard IEEE 1363.1) [25], заснована на задачі згортки модулярних решіток (Convolution modular lattice, CML), з публічним ключем довжини $n\log n$, що стала стандартом шифрування.

Розглянемо алгоритм асиметричного шифрування, що реалізує цифровий підпис із складністю $O(n^2)$, розмірами закритого, відкритого ключа та сертифіката $\tilde{O}(n)=m\log q$, що заснований на циклічних решітках.

Нехай єдайджест геш-функції $A=[A^{(1)}|\cdots|A^{(m/n)}]$ зі складністю $O(n)$; публічний ключ – $X=h_a(x)$ $=\sum A^{(i)}x^{(i)}$, $\mathrm{Y}=\mathrm{h}_a(y)\sum A^{(i)}y^{(i)}$; закритий ключ - $x=[x^1,\cdots,x^{(m/n}]$, $y=[y^1,\cdots,y^{(m/n)}]$.

Генерація підпису для n-бітів даних $m\in\{0,1\}^n$ реалізується за допомогою обчислення: $\sigma=(\sigma_1,\cdots,$ $\sigma_{m/n})$, де $\sigma_i=x^{(i)}M+y^{(i)}$ і M представлено у виді матриці:

$$\mathrm{M}=\begin{bmatrix} m_1 & -m_1 & \cdots & -m_2 \\ m_2 & m_1 & \cdots & -m_3 \\ \vdots & \vdots & \ddots & \vdots \\ m_n & m_{n-1} & \cdots & m_1 \end{bmatrix}.$$

Перевірка підпису полягатиме у обчисленні $h_a(\sigma)=XM+Y$.

Для широкого класу ймовірнісних варіантів задач теорії решіток, на яких засновані системи Ajtai-Dwork та GGH, було продемонстровано сильний алгоритм атаки, що дозволяє реалізувати атаку закритого ключа [26]. У цій же роботі було продемонстровано метод захисту від атаки.

На конференції Єврокрипт 2006 [27] було експериментально продемонстровано вразливість шифрування із встановленими стандартом параметрами для систем шифрування GGH та NTRU. Було продемонстровано атаку на банківські смарт-картки та системи ідентифікації особистості, що захищені криптографічною системою NTRU. Складність розв'язання задач теорії решіток визначається вибором розмірності та базису решітки. Вибір решітки великої розмірності збільшує потужність ключового простору, але зростання цього параметра утрудняється швидким зростанням обсягу даних, необхідних для зберігання ключів і збільшення часу шифрування /дешифрування. Для кожної із систем про зростання часу потрібно говорити окремо, в силу специфічних властивостей шифрування. Наприклад, публічний ключ 1000-мірної решітки в системі Ajtai-Dwork'a займе 84 Гб, в GGH 290 Мб і 50 Мб для NTRU, при цьому розмір закритого ключа значно більший. Вибір базису обґрунтований типом задач, що лежить в основі шифрування.

Приведемо порівняння асиметричних систем шифрування класу $NPcoNP$ (RSA та ECC) та системи шифрування на основі модулярних решіток NTRU (табл. 1), де МІПС – мільйон цілих інструкцій за рік; таблиця складена з урахуванням відомостей співтовариства NTRU, стандарт IEEE 1363.1. Розмір ключа шифрування NTRU та зростання складності шифрування /дешифрування зі зростанням криптостійкості зростає повільніше, ніж у RSA. Зростання складності шифрування/дешифрування системи NTRU росте повільніше, ніж у криптографії на основі еліптичних кривих ECC.

Таблиця 1

Порівняння асиметричних систем шифрування класу $NPcoNP$ та системи шифрування

Потужність ключевого простору в бітах	Розмір відкритого ключа в бітах			Час атаки в МІПС за рік
	NTRU	ECC	RSA	
80	2008	160	1024	10^{12}
112	3033	224	2048	$5\cdot10^{21}$
128	3501	256	3072	$3\cdot10^{26}$
160	4383	320	4096	$22\cdot10^{33}$
256	7690	521	15360	$1{,}8\cdot10^{62}$

ВИСНОВКИ

В статті розглядається проблема аналізу, дослідження, оцінки та порівняння кандидатів на

постквантові стандарти ЕП з використанням математики алгебраїчних решіток, а також розробки рекомендацій щодо вибору із них найбільш перспективних для майбутнього застосування.

Робота містить необхідні базові визначення, опис основних задач теорії алгебраїчних решіток, а також представлені основні переваги цього класу криптографії – властивість криптостійкості по відношенню до квантових обчислювачів. Вперше сутність криптоперетворення на алгебраїчних решітках у 1996 році запропонував M. Aitai.

Задачі теорії решіток надають широкі можливості реалізації криптографічних протоколів і примітивів, а також торкаються безлічі фундаментальних питань, починаючи від задач лінійного програмування до узагальнених теоретико-числових проблем. Побудова криптографічних систем на основі задач теорії решіток неможлива без подальшого дослідження перерахованих вище задач і алгоритмів їх розв'язку. Тому вивчення та уточнення властивостей задач теорії решіток - це одна з основних цілей як при побудові, так і при криптоаналізі примітивів і протоколів на основі задач теорії решіток. Важливість цього напряму досліджень обумовлена також наявністю у задач теорії решіток (при деяких параметрах) властивостей криптостійкості до алгоритмів, що виконуються на квантових комп'ютерах.

Одним із важких виборів, з якими стикнувся NIST при визначенні ефективності обчислень, було прийняття рішення між Kyber, NTRU та Saber. Усі троє були обрані фіналістами і були дуже порівнянні один з одним. NIST впевнений у безпеці, яку забезпечує кожен. Більшість додатків зможуть використовувати будь-яку з них без суттєвих штрафів на продуктивність. Як зазначається, на завершення 2-го раунду NIST мав намір стандартизувати лише один із цих фіналістів, оскільки всі троє базувалися на структурованих решітках. Проблеми, пов'язані з патентами, були фактором рішення NIST протягом 3-го раунду, оскільки NIST дізнався про різні сторонні патенти. Однією з відмінностей між Kyber, Saber та NTRU є конкретне припущення щодо безпеки, що кожен покладається на безпеку. NIST вважає проблему MLWE, від якої залежить Kyber, трохи переконливішою, ніж інші припущення, такі як MLWR або проблема NTRU. NIST також високо оцінив специфікацію команди Kyber, яка включала ретельний і детальний аналіз безпеки. Що стосується продуктивності, то Kyber був майже найкращим (якщо не найкращим) у більшості тестів.

ЛІТЕРАТУРА

[1]. Alagic G., Alperin-Sheriff J., et al. (2019) Status report on the first round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8240. Режим доступу: https: // doi.org/10.6028/ NIST.IR.8240.

[2]. Alagic G., Alperin-Sheriff J., et al. (2020) Status report on the second round of the NIST post-quantum cryptography standardization process (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8309. Режим доступу: https://doi.org /10.6028/NIST.IR.8309.

[3]. NIST PQC. [Elektronnyi resurs]. Rezhym dostupa: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[4]. Schank J. (2021) Category 5 NTRU parameters. [Elektronnyi resurs]. Rezhym dostupa: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/t1-JCgzSS-uk/m/VXXQaJgFCQAJ.

[5]. National Institute of Standards and Technology (2016) Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. [Elektronnyi resurs]. Rezhym dostupa: https: // csrc.nist.gov /CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[6]. Єсіна М.В. Стан третього раунду процесу стандартизації постквантової криптограрафії NIST / М.В. Єсіна, Є.В. Острянська, І.Д. Горбенко. Radiotekhnika. No. 210 (2022). С. 75-86.

[7]. Bernstein D., Lange T. (eds.), eBACS: ECRYPT Benchmarking of Cryptographic Systems – SUPERCOP (2020). [Elektronnyi resurs]. Rezhym dostupu: https://bench.cr.yp.to/supercop.html.

[8]. 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.

[9]. Ajtai M. Generating Hard Instances of Lattice Problem. Proc. of 28th ACM Symp. on Theory of Comp. Philadelphia: ACM Press. 1996. pp. 99-108.

[10]. Post-Quantum Cryptography PQC. Round 3 Submissions. NIST Computer Security Resource Center (CSRC). Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

[11]. PQC Standardization Process Third Round Candidate Announcement. NIST Computer Security Resource Center (CSRC). July 22, 2020. Rezhym dostupa: https: // csrc.nist.gov / News / 2020/pqc-third-round-candidate-announcement.

[12]. Boas. P. Another NP-complete problem and the complexity of computing short vectors in a lattice",

Tech. Report 81-04, Math Inst. Univ. Amsterdam, 1981.
[13]. Impagliazzo R., A personal view of average-case complexity. Proceeding of 10th IEEE Annual Conference on Structure in Complexity Theory, 1995, pp. 134-147.
[14]. Cai J.Y., Nerurkar A. P. An improved Worst-case to Average case reduction for lattice problems. FOCS. 1997. pp. 468-477.
[15]. Micciansio D., Regev O. Worst-case to average-case reduction based on Gaussian measures. FOCS. 2004. pp. 372-381.
[16]. Goldreich O., Goldwasser S., Halevi S. Collision-free hashing from lattice problems. Technical Report TR96-056. Electronic Colloquium on Computation Complexity (ECCC). 1996.
[17]. D. Deutsch, Quantum computational networks, Proc. Roy. Soc. London, Ser A, 425, pp. 73-90, 1989.
[18]. Lyubashevsky V., Micciancio. On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem. Lecture Notes in Computer Science. №5677. 2009. pp. 577-594.
[19]. Micciancio D., Vadhan S. Statistical zero-knowledge proofs with efficient provers: lattice problems and more. In Advances in cryptology. Lecture Notes in Computer Science. 2003. pp. 282-298.
[20]. Micciancio D. The shortest vector problem is NP-hard to approximate to within some constant. SIAM J. CS. №30. 2001. pp. 2008-2035.
[21]. Weiss A. Shortest Vector in A Lattice is NP-Hard to approximate. The Hebrew University of Jerusalem. Inapproximability Seminar, Spring 2005, http: // www.cs.huji.ac.il/inapprox/papers/SVP-micc.pdf.
[22]. Celebi M. E., Celiker F., Kingravi H. A.On Euclidean Norm Approximations. http: // arxiv.org / abs/ 1008.4870
[23]. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In Proc. 40th ACM Symp. on Theory of Computing (STOC). 2008. pp. 197-206.
[24]. Goldreich O, Goldwasser, Halevi S. Public-key cryptosystems from lattice reduction problems. In Advances in cryptology. Lecture Notes in Computer Science. – №1294. 1997. pp. 112-131.
[25]. Peikert C., Vaikuntanathan V. Noninteractive statistical zero-knowledge proofs for lattice problems. In Advances in cryptology (CRYPTO), LNCS. Springer. №5157. 2008. pp. 536-553.
[26]. Peikert C., Vaikuntanathan V., Waters B. A framework for efficient and composable oblivious transfer. LNCS. №5157. 2008. p. 554-571.
[27]. Lyubashevsky V. Lattice-based identification schemes secure under active attacks. In PKC. №4939. 2008. pp. 162-179.

MATHEMATICAL FUNDAMENTALS OF ALGEBRAIC GRIDS AND THEIR APPLICATION IN QUANTUM CRYPTOLOGY

The ongoing development of quantum computers threatens state-of-the-art public key cryptographic schemes, such as discrete logarithm factorization key generation schemes, digital signatures, and elliptic curve cryptography. It is necessary to develop new cryptographic algorithms capable of resisting the attacks of quantum computers. Post-quantum cryptography (PQC) aims to develop algorithms that can be used without significant modifications to existing networks. The US National Institute of Standards and Technology (NIST) organizes a competition for the selection and standardization of new algorithms. This article provides an overview and analysis of the evaluation and selection process of NIST algorithms based on lattice theory problems. It gives basic definitions, describes the main problems of algebraic lattice theory, and summarizes the advantages of this class of cryptography, including its resistance to quantum computing. The work contributes to the study and comparison of post-quantum cryptographic algorithms, and also provides recommendations for their further use and standardization to ensure their security in the development of quantum computers.

Keywords: post-quantum cryptography, algebraic lattices, quantum computers, cryptographic algorithms, lattice theory, standardization of cryptography.

Кожухівський Андрій Дмитрович, д-р техн. наук, професор, Державний університет інформаційно-комунікаційних технологій, професор кафедри інформаційної та кібернетичної безпеки; Київ; Україна.

Andriy Kozhukhivskyi, Dr. Tech. Sciences, professor, State University of Information and Communication Technologies, professor of the department of information and cybernetic security, Kyiv, Ukraine.
E-mail: akozhuh@gmail.com.
Orcid ID: 0000-0002-1725-2365.

Хіміч Олександр Миколайович, д-р фіз.-мат. наук, акад. НАНУ, заступник директора Інституту Кібернетики ім. В.М. Глушкова НАНУ.

Oleksandr Khimich, Dr. Phys.-Math. of Sciences, Acad. NASU, deputy director of the Institute of Cybernetics named after V.M. Hlushkova National Academy of Sciences.
E-mail: khimich505@gmail.com.
Orcid ID: 0000-0002-8103-4223.

Потій Олександр Володимирович, д-р техн. наук., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України.

Oleksandr Potii, Dr. Tech. Sci., professor, deputy head of the State Service for Special Communications and Information Protection of Ukraine.
E-mail: potav@ua.fm.
Orcid ID: 0000-0002-2366-0541.

Горбенко Юрій Іванович, канд. техн. наук, АТ «Інститут інформаційних технологій», перший заступник головного конструктора, Україна.

Yuriy Horbenko, candidate. technical of Sciences, JSC "Institute of Information Technologies", first deputy chief designer, Ukraine.
E-mail: gorbenkou@iit.kharkov.ua.
Orcid ID: 0000-0003-0073-9107.

Кожухівська Ольга Андріївна, д-р техн. наук, Державний університет інформаційно-комунікаційних технологій, доцент кафедри інформаційної та кібернетичної безпеки; Київ, Україна.

Olga Kozhuhivska, Dr. Tech. of Sciences, State University of Information and Communication of technologies, associate professor of the department of information and cybernetic security, Kyiv, Ukraine.
E-mail: rsg.o.i.v@gmail.com.
Orcid ID: 0009-0008-2176-9149.

Борсуковський Юрій Володимирович, канд. техн. наук, Державний університет інформаційно-комунікаційних технологій, доцент кафедри інформаційної та кібернетичної безпеки; Київ; Україна.

Yuryi Borsukovskiy, Candidate of Sciences. technical Sciences, State University of Information and Communication Technologies, associate professor of the department of information and cybernetic security, Kyiv, Ukraine.
E-mail: gmbyurii@gmail.com.
Orcid ID: 0000-0003-1973-2386.

DOI: 10.18372/2410-7840.26.18836
УДК 004.056.53

ОБҐРУНТУВАННЯ ІМОВІРНОСТІ УНЕМОЖЛИВЛЕННЯ ВИЗНАЧЕННЯ НАЯВНОСТІ СИГНАЛІВ В СЕРЕДОВИЩАХ ЇХ ПОШИРЕННЯ

Сергій Іванченко, Василь Некоз

Проведено обґрунтування унеможливлення визначення наявності сигналів в середовищах їх поширення В якості моделі каналу розповсюдження інформації було використано дискретно-неперервний канал. Інформація вироблялась від дискретного джерела, де кожному з інформаційних символів ставились у відповідність неперервні реалізації, які поширювались неперервним середовищем із завадою. Прийом сигналів здійснюється засобами, які можуть бути ефективними. З точки зору убезпечення інформації від неконтрольованого порширення та забезпечення її захищеності в середовищі поширення, як правило, використовують два фактори: згасання амплітуди хвилі (сигналу) при її поширенні у фізичному середовищі; спотворююча дія завади, що має місце в середовищі поширення сигналу та руйнує його форму. Однак, використання цих факторів, що могло б забезпечити повну, майже абсолютну безпеку інформації, є питанням складним, а то і неможливим. Адже сигнали, що поширюються у просторі, відповідно до законів фізики здійснюють це у вигляді електромагнітних чи інших хвиль, або потоків елементарних (заряджених) частинок. Вони можуть поширюватись на досить великі відстані, а теоретично майже до нескінченності, ефективність перехоплення яких повністю визначається ефективністю засобів прийому. Для вирішення зазначеного питання, що має широке застосування у менеджменті інформаційної безпеки, є ризик орієнтований підхід, який не вимагає абсолютного убезпечення, а допускає можливість не виконання вимоги з безпеки з деяким певним допустимим ризиком [2]. Цей ризик, як правило, визначається допустимими збитками, які може понести власник активів, і при цьому результативність виробничих процесів не порушиться.

***Ключові слова**: інформаційна безпека, кібербезпека, інформаційно-комунікаційні системи, системи захисту інформації, інформаційний сигнал, дискретний канал.*

ВСТУП

Забезпечення ризику в каналах витоку вимагає вирішення актуального завдання, а саме обґрунтування сукупності взаємозв'язаних показників, які мають надати можливість трансформування захищеності від ризику безпеки до енергетичних умов в середовищі поширення.

Паралельно при цьому одним із основних питань є обґрунтування зв'язку імовірності неможливості впевненого визначення ознак інформаційного сигналу та граничного відношення сигнал/завада, яке також вимагає окремого вирішення.

ОСНОВНА ЧАСТИНА

Обґрунтування сукупності показників для забезпечення безпеки інформації від неконтрольованого поширення на основі унеможливлення визначення ознак інформаційних сигналів

Зазначені показники повинні забезпечити виконання вимоги з захищеності інформації від неконтрольованого поширення в усіх можливих середовищах, та мати поміж собою зв'язок, який би дозволяв стверджувати про еквівалентність цих показників з допустимим ризиком безпеки – ступенем невиконання вимог. Нехай задано якісну вимогу, якою є неможливість визначення оз-