УДК 511.7

Ліхачов А. Д., Олійник Б. В.

DOI: 10.18523/2617-7080720243-8

СХЕМА РОЗПОДІЛУ СЕКРЕТУ, ЩО БАЗУЄТЬСЯ НА КРИПТОСИСТЕМІ ГОЛДВАССЕР-ГОЛДРІХА-ХАЛЕВІ

З розвитком квантових технологій стає актуальним питання про дослідження та впровадження криптографічних примітивів, що базуються на складних задачах для квантових обчислень. Такі криптографічні примітиви є стійкими щодо квантового криптоаналізу. Прикладом задач, що мають експоненційну складність для квантових обчислень, є задачі на решітках, такі як пошук найкоротшого вектора або пошук найближчого вектора. Однією з перших і найвідоміших квантово-стійких криптосистем, що в основі свого математичного апарату використовує задачі на решітках, є криптосистема Голдвассер-Голдріха-Халеві.

Схема розподілення секрету є фундаментальним криптографічним примітивом, що допускає розподілення секрету між множиною учасників, при цьому відновлення секрету можливе тільки при авторизації всіх або певної частини учасників (порогу учасників). Також необхідною умовою схеми розподілення секрету є неможливість окремих учасників, або груп учасників, кількість яких менша за поріг, відновити секрет.

Варіанти побудови схем розподілу секрету на різних математичних моделях, у тому числі на решітках, наразі активно досліджуються, оскільки вони дозволяють проводити надійні багатосторонні обчислення, безпечно поширювати інформацію шляхом поширення і розподілення оригіналу даних між різними серверами, для побудови компіляторов схем із захистом від витоку тощо. У цій роботі запропоновано нову квантово-стійку n-порогову схему розподілу секрету для n учасників, що базується на криптосистемі Голдвассер-Голдріха-Халеві.

Ключові слова: цілочисельна решітка, алгоритм Бабаї, криптосистема Голдвассер-Голдріха-Халеві, схема розподілу секрету, асиметричний алгоритм шифрування.

Вступ

З розвитком квантових технологій виникає потреба в дослідженнях та впровадженнях криптографічних примітивів, що базуються на складних задачах для квантових обчислень. Такі криптографічні примітиви є стійкими щодо квантового криптоаналізу. Прикладом задач, що є складними для квантових обчислень (тобто мають експоненційну складність), є задачі на решітках, такі як пошук найкоротшого вектора або пошук найближчого вектора. Однією з перших і найвідоміших квантово-стійких криптосистем, яка в основі свого математичного апарату використовує задачу на решітках, є криптосистема Голдвассер-Голдріха-Халеві [3; 4; 10].

Схема розподілення секрету [8] є фундаментальним криптографічним примітивом, що допускає розподілення секрету між множиною учасників, при цьому відновлення секрету можливе тільки при авторизації всіх або певної частини учасників (порогу учасників). Також необхідною умовою схеми розподілення секрету є неможливість окремих учасників, або груп учасників, кількість яких менша за поріг, відновити секрет.

Схеми розподілення секрету використовуються для надійних багатосторонніх обчислень, для побудови компіляторов схем із захистом від витоку [2; 5], для аутсорсингу даних у безпечний спосіб, що дозволяє уникнути необхідності витрачати час на процес шифрування та дешифрування і проблем, які пов'язані з управлінням ключами [9], тощо. Варіанти побудови схем розподілу секрету на різних математичних моделях[2], у тому числі й на решітках [7], наразі активно досліджуються різними науковцями. У цій роботі запропоновано нову n-порогову схему розподілу секрету для n учасників, що базується на криптосистемі Голдвассер-Голдріха-Халеві.

Необхідні визначення

Спочатку нагадаємо основні означення.

Означення 1. [10] Нехай $v_1, \ldots, v_n \in \mathbb{R}^m$ є множиною лінійно незалежних векторів. Решіткою L, породженою $v_1, \ldots, v_n$, називають множину всіх лінійних комбінацій $v_1, \ldots, v_n$ з цілими коефіцієнтами, тобто

$$L = \{a_1v_1 + a_2v_2 + \ldots + a_nv_n \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

«Поганим» базисом решітки L називають менш ортогональний її базис. Відповідно,

«хорошим» базисом решітки є її ортогональний базис або подібний до ортогонального.

Основними задачами на решітках, які є «складними», тобто мають експоненційну складність для звичайних і квантових обчислень, і які використовують у криптографії, є пошук найкоротшого вектора, пошук найближчого вектора та пошук найменшого базису.

Наведемо формулювання цих задач.

Означення 2. [10] Задачу пошуку найкоротшого вектора (Shortest Vector Problem, SVP) у решітці L можна описати одним із трьох таких способів:

- знайти ненульовий вектор x у решітці L, для котрого
$$\|x\| \leq \|y\|$$
для всіх ненульових $y \in L$, тобто $\|x\| = \lambda_1(L)$;
- SVP_γ: знаходження апроксимованого найменшого вектора x у решітці L, який
$$\|x\| \leq \gamma \cdot \lambda_1(L),$$
для малої константи γ;
- $uSVP_\gamma$: для константи $\gamma > 1$ та решітки L таких, що
$$\lambda_2(L) > \gamma \cdot \lambda_1(L),$$
знайти такий ненульовий вектор $x \in L$ довжини $\lambda_1(L)$.

Означення 3. [10] Маючи решітку L у n-вимірному дійсному просторі та $x \in \mathbb{R}^n, x \notin L$, проблему пошуку найближчого вектора (Closest Vector Problem, CVP) можна описати так:

- знайти такий вектор $y \in L$, щоб
$$\|x - y\| \leq \|x - z\|$$
для всіх $z \in L$;
- CVP_γ: знайти такий y, щоб
$$\|x - y\| \leq \gamma \cdot \|x - z\|$$
для всіх $z \in L$ та малої константи γ.

Означення 4. [3] Проблема пошуку найменшого базису (Smallest Basis Problem, SBP) : маючи базис B решітки L, треба знайти інший базис B' для цієї самої решітки, у якому добуток довжин його елементів буде найменшим.

Наведені задачі мають експоненційну складність для звичайних і для квантових обчислень. В загальному випадку наразі не існує алгоритму, за яким можливо було б знайти розв'язки за поліноміальний час, проте для ортогонального базису існують алгоритми, що працюють швидко. Найшвидші алгоритми для розв'язання наведених задач, які перераховані вище, досягають експоненційних множників і базуються на алгоритмі LLL [10]. Алгоритм LLL використовують для знаходження апроксимованого розв'язку задач пошуку найкоротшого вектора та найменшого базису. Для знаходження наближеного розв'язку задачі пошуку найближчого вектора — підхід Бабаї [10] з використанням змінених базисів.

Зауважимо також, що задачі SVP, CVP та SBP є NP–складними задачами [6].

Алгоритм Бабаї

Алгоритм Бабаї [1] використовують для знаходження найближчого вектора (CVP) з наближенням $\gamma = 2^{(n-2)/2}$ за експоненційним часом. Опишемо кроки цього алгоритму.

Нехай $b_1, b_2, \ldots, b_m$ є базисом решітки $L \subset \mathbb{R}^n$ та нехай $x \in \mathbb{R}^n$ є довільним вектором, відстань до якого необхідно знайти. Для цього алгоритму базисні вектори мають бути ортогональними. Якщо вони не є такими, доречним буде застосувати алгоритм LLL [10], який здійснює зміну базису до більш ортогонального. Задачу пошуку найближчого вектора розв'язує такий алгоритм [4]:

1. Визначають рівняння
$$x = t_1 b_1 + t_2 b_2 + \ldots + t_n b_n,$$
у якому коефіцієнти $t_1, t_2, \ldots, t_n \in \mathbb{R}$.
2. Знаходять розв'язок рівняння та призначають $a_i = \lfloor t_i \rceil$ для $i = 1, 2, \ldots, n$.
3. Знаходять вектор y у решітці L, наближений до вектора x:
$$y = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n.$$

Криптосистема Голдвассер-Голдріха-Халеві

У цьому розділі ми наведемо опис криптосистеми з відкритим ключем Голдвассер-Голдріха-Халеві (GGH), яка є однією з перших і найвідоміших криптосистем, що базуються на складних задачах на решітках [3; 4; 10]. Для кращого розуміння, як працює криптосистема, ми опишемо процес шифрування, надсилання і дешифрування інформації як процес обміну інформацією між Алісою та Бобом [4].

Аліса обирає набір лінійно незалежних майже ортогональних між собою векторів
$$v_1, v_2, \ldots, v_n \in \mathbb{Z}^n.$$
Цей набір векторів V вважається «хорошим» базисом, який лежить в основі решітки L та є приватним ключем Аліси. Наступним кроком

генерується випадковим чином матриця U з цілими коефіцієнтами та $det(U) = \pm 1$. Генерування цієї матриці випадковим чином необхідно для знаходження набору векторів, який буде «поганим» базисом — публічним ключем Аліси. Одним із способів отримання матриці U є множення великої кількості випадково обраних елементарних матриць.

$$W = UV$$

Отже, ряд векторів $w_1, w_2, \ldots, w_n$ є новим базисом решітки L та є публічним ключем Аліси.

Тепер припустимо, що Боб хоче переслати повідомлення Алісі. До свого повідомлення m, яке також має векторну форму та може мати вигляд бінарного вектора, Боб додає малий вектор збурення r, який є також ефімерним (сесійним) ключем. Наприклад, координати вектора r можуть бути випадково обрані між δ та $-\delta$, де δ сталий публічний параметр. Далі відбувається процес шифрування:

$$e = mW + r = \sum_{i=1}^{m} m_i w_i + r,$$

де e — шифротекст, та $e \notin L$, але максимально наближений до точки $mW \in L$.

Процес дешифрування відбувається таким чином. Аліса застосовує алгоритм Бабаї з «хорошим» базисом $v_1, v_2, \ldots, v_n$, щоб знайти вектор у решітці L, який буде найближчим до вектора шифротексту e. Враховуючи те, що вона використовує «хороший» (а отже й ортогональний) базис, а вектор збурення r є малим, вектор решітки, який знаходить Аліса, являє собою mW. Помножуючи його на W^{-1}, вона знаходить оригінальне, дешифроване повідомлення від Боба m.

Схема розподілу секрету

Сформулюємо строге означення схеми розподілення секрету. Для цього спочатку нагадаємо визначення k-монотонної структури доступу і визначимо функцію розподілу доступу.

Означення 5 (**k-монотонна схема доступу**)**.** [9] Схема доступу A є монотонною, якщо для будь-якої множини $S \in A$ будь-яка надмножина S також є в A. Ми будемо називати таку схему доступу k-монотонною, якщо для будь-якої множини $S \in A$ буде виконуватись $|S| \geq k$.

Означення 6 (**Функція розподілення доступу**)**.** [9] Нехай $[n] = 1, 2, \ldots, n$ буде множиною ідентичностей n сторін. Нехай M буде областю секретів. Функція розподілення доступу $Share$ — це рандомізоване відображення з M на $S_1 \times S_2 \times \ldots \times S_n$, де S_i є областю поширень сторони з ідентичністю i. Для множини $T \subseteq [n]$ ми визначимо $Share(m)_T$ як обмеження для $Share(m)$ для її T записів.

Означення 7 (**$(A, n, \varepsilon_c, \varepsilon_s)$-Схема розподілення секрету**)**.** Нехай M скінченна множина секретів, де $|M| \geq 2$. Нехай $[n] = 1, 2, \ldots, n$ множиною ідентичностей для n сторін. Функція поширення $Share$ із областю секретів M являє собою $(A, n, \varepsilon_c, \varepsilon_s)$–схему розподілення секрету відносно монотонної схеми доступу A, якщо виконуються такі дві вимоги:

- **Коректність:** секрет може бути відновленим будь-якою множиною сторін, які є частиною схеми доступу A. Тобто для будь-якого набору $T \in A$ існує детермінована функція відновлення $Rec : \otimes_{i \in T} S_i \to M$ така, що кожне $m \in M$,

  $$Pr[Rec(Share(m)_T) = m] = 1 - \varepsilon_c$$

  де ймовірність перевищує випадковість функції $Share$.
- **Статистична конфідеційність:** будь-яке об'єднання сторін, які не є частиною схеми доступу, не повинно мати майже жодної інформації про основний секрет. Тобто для будь-якої неавторизованої множини $U \subseteq [n]$, такої, щоб $U \notin A$, а також для кожної пари секретів $m_0, m_1 \in M$, для кожного обчислювально необмеженого розрізнювача D зі значенням $\{0, 1\}$ має місце таке:

  $$|Pr[D(Share(m_0)_U) = 1] - Pr[D(Share(m_1)_U) = 1]| \leq \varepsilon_s.$$

Визначимо швидкість схеми розподілення секретами як

$$lim_{|m| \to \infty} \frac{|m|}{max_{i \in [n]} |Share(m)_i|}.$$

Означення 8 (**Порогова схема розподілення секрету**)**.** Визначимо t-порогову схему як $(t, n, \varepsilon_c, \varepsilon_s)$-схему розподілення секрету.

Узагальнюючи, схема розподілення секрету для певної схеми доступу та осіб складається з функцій $Share$, яка розподіляє секрет між учасниками схеми доступу, та Rec (Recombine), яка відновлює секрет для певної множини учасників, якщо їх кількості достатньо для відновлення секрету. Поріг схеми розподілення секрету (t, n) визначає, що секрет може бути відтворений t кількістю учасників із загальної кількості n.

Також, схему розподілу секрету вважають безпечною, якщо жоден нескінченно потужний

нападник не може нічого дізнатися про основний секрет, не маючи доступу до монотонної схеми доступу A. Насправді, такі схеми вважають інформаційно-теоретично захищеними, але ми просто називатимемо такі схеми безпечними.

Зараз ми продемонструємо можливість зберігання та відтворення секрету, використовуючи криптосистему Голдвассер-Голдріха-Халеві, яка була описана вище. Нова побудована схема буде n-пороговою, тобто (n, n), а отже відновлення секрету буде можливим лише за умови наявності всіх n сторін.

Кількість базисних векторів решітки напряму залежить від кількості учасників нашої схеми. Нехай ми маємо n учасників. Виберемо цілочисельну решітку L, базис якої складається з n векторів. Позначимо через $v_1, v_2, \ldots, v_n$ лінійно незалежні майже ортогональні вектори, що утворюють решітку L, тобто «хороший» базис нашої решітки.

Секрет, який має бути розподіленим поміж сторонами, позначимо як S. Секрет також має векторний вигляд. Шифруємо його таким чином:

$$S_{enc} = SW + r = \sum_{i=1}^{S} S_i w_i + r,$$

де r — малий вектор збурення, який є також ефімерним ключем.

Кожній стороні схеми видається комбінація (v_i, S_{enc}). Коли всі учасники схеми збирають свої комбінації, ми отримуємо повний «хороший» базис, тоді секрет S можна відновити з допомогою алгоритму Бабаї.

Знаходимо вектор у решітці L, який буде найближчим до вектора S_{enc}. Враховуючи те, що ми маємо «хороший» базис і публічний вектор збурення r є малим, вектор решітки, який ми знаходимо, являє собою SW. Помножуючи його на W^{-1}, ми відновлюємо оригінальний секрет S.

Також можна сформулювати таку теорему.

Теорема 1. *Схема розподілу секрету на основі криптосистеми Голдвассер-Голдріха-Халеві є коректною та статистично конфіденційною.*

Доведення. Розглянута схема є (n, n) пороговою, кожен учасник котрої має пару (v_i, S_{enc}), де v_i — частка лінійно незалежного ортогонального базису (приватного ключа) V, а S_{enc} — зашифрований секрет.

Схема розподілення секрету є коректною, оскільки

$$Pr[Rec(Share(S)_T) = m] = 1,$$

тобто секрет відновлюється з імовірністю 1 тоді і тільки тоді, коли наявний повний «хороший» базис, а це можливо тоді і тільки тоді, коли множина сторін n є повною, тобто наявні всі n сторін.

Схема є також статистично конфіденційною, оскільки за наявності меншої кількості учасників, ніж n, для відновлення секрету потрібно «доповнити»базис до n векторів, вибравши якимось чином вектори, ких не вистачає. При цьому, оскільки базис решітки L складається з n векторів, кожен вектор має не менше ніж n координат. Таким чином у випадку наявності пари секретів m_0 та m_1, навіть $n-1$ кількість учасників не матимуть можливість зрозуміти, до якого секрету відносяться наявні в них ключі, оскільки частинами ключів є пари (v_i, S_{enc}), а сукупність навіть $n-1$-го вектора v_i не дає можливість розшифрувати секрет. А тому вгадати, який саме з двох секретів був зашифрований, можна однаковою ймовірністю, близькою до $\frac{1}{2}$.

Як приклад розглянемо схему з трьома учасниками. Маємо такі три базисні вектори, що формують решітку L:

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}, v_3 = \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}.$$

Вони є «хорошим» базисом V.

Маємо секрет $S = (240, 80, 1991)$ і вектор збурення $r = (1, 0, -1)$. Шифруємо наш секрет:

$$S_{enc} = SW + r = \\ = (240, 80, 1991) \begin{pmatrix} 6 & 3 & 3 \\ 3 & 0 & 3 \\ 1 & -1 & -4 \end{pmatrix} + (1, 0, -1) = \\ = (3671, -1271, -7004).$$

Кожен із трьох учасників схеми отримує свою пару (v_i, S_{enc}):

- перший учасник отримує

$$(\begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, (3671, -1271, -7004));$$

- другий учасник отримує

$$(\begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}, (3671, -1271, -7004));$$

- третій учасник отримує

$$(\begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}, (3671, -1271, -7004)).$$

Для відновлення секрету застосуємо алгоритм Бабаї. Ми шукатимемо найближчий вектор решітки із базисними векторами V до S_{enc}. Запишемо S_{enc} у вигляді

$$S_{enc} = t_1 v_1 + t_2 v_2 + t_3 v_3,$$

отже отримуємо

$$\begin{pmatrix} 3671 \\ -1271 \\ -7004 \end{pmatrix} = t_1 \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} + t_2 \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix} + t_3 \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix},$$

розв'язуючи це рівняння знаходимо

$$t_1 = -1431 = a_1, t_2 = 2231 = a_2, t_3 = 320 = a_3.$$

Далі обчислюємо

$$y = a_1 v_1 + a_2 v_2 + a_3 v_3$$

та отримуємо:

$$y = -1431 \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} + 2231 \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix} + 320 \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3671 \\ -1271 \\ -7004 \end{pmatrix},$$

y буде найближчим вектором до S_{enc}. Тепер, щоб відновити секрет S, треба обчислити yW^{-1}:

$$S = yW^{-1} = (3671, -1271, -7004) \times \times \frac{1}{18} \begin{pmatrix} 1 & 3 & 3 \\ 5 & -9 & -3 \\ -1 & 3 & -3 \end{pmatrix} = \begin{pmatrix} 240 \\ 80 \\ 1991 \end{pmatrix}$$

Отриманий дешифрований результат збігається з первинним секретом.

Список літератури

1. Babai L. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 1986, Vol. 6. Pp. 1–13. https://doi.org/10.1007/BF02579403.
2. Binu V. P., Sreekumar A. Simple and Efficient Secret Sharing Schemes for Sharing Data and Image. *International Journal of Computer Science and Information Technologies*. 2015. Vol. 6 (1). Pp. 404–409.
3. Goldreich O., Goldwasser S., Halevi S. Publickey cryptosystems from lattice reduction problems. *Proceedings of 17th Annual International Cryptology Conference*. Santa Barbara, California, USA, 1997. Pp. 112–131.
4. . Junying Liang, Haipeng Peng, Lixiang Li, Fenghua Tong, Shuang Bao, Lanlan Wang. A secure and effective image encryption scheme by combining parallel compressed sensing with secret sharing scheme. *Journal of Information Security and Applications*. 2023. Vol. 75. 103487. https://doi.org/10.1016/j.jisa.2023.103487.
5. Hoffstein J., Pipher J., Silverman J. H. An Introduction to Mathematical Cryptography. Springer Science+Business Media, LLC, 2016.
6. Nguyen P. Cryptoanalysis of the Goldreich–Goldwasser–Halevi Cryptosystem from Crypto'97. *Advances in Cryptology — CRYPTO' 99. Lecture Notes in Computer Science*. Vol. 1666, Springer, Berlin, 1999. Pp. 288–304. https://doi.org/10.1007/3-540-48405-1_18.
7. Ravi P., Howe J., Chattopadhyay A., Bhasin S. Lattice-Based Key Sharing Schemes: A Survey. *ACM Computing Surveys*. 2021. Vol. 54, Issue 1, Article No. 9. Pp. 1–39.
8. Shamir A. How to share a secret. *Communications of the Association for Computing Machinery*. 1995. Vol. 22, No. 11. Pp. 612–613.
9. Srinvasan A., Vasudevan P. N. Leakage Resilient Secret Sharing and Applications. *Advances in Cryptology — CRYPTO' 2019. Lecture Notes in Computer Science*. Vol. 11693. Springer, Berlin, 2019. Pp. 480–509.
10. Smart N. P. Cryptography Made Simple. Springer International Publishing Switzerland, 2016.

References

1. L. Babai, Combinatorica. **6**, 1–13 (1986), https://doi.org/10.1007/BF02579403.
2. V. P. Binu and A. Sreekumar, International Journal of Computer Science and Information Technologies. **6** (1), 404–409 (2015).
3. O. Goldreich, S. Goldwasser, and S. Halevi, in: *Proceedings of 17th Annual International Cryptology Conference*(Santa Barbara, California, USA, 1997), pp. 112–131.
4. J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography* (Springer Science+Business Media, LLC, 2016).
5. Junying Liang, Haipeng Peng, Lixiang Li, Fenghua Tong, Shuang Bao, and Lanlan Wang, Journal of Information Security and Applications. **75** (2023), 103487. https://doi.org/10.1016/j.jisa.2023.103487.
6. P. Nguyen, in: *Advances in Cryptology—CRYPTO' 99. Lecture Notes in Computer Science*, Vol. 1666 (Springer, Berlin, 1999), pp. 288–304. https://doi.org/10.1007/3-540-48405-1_18.
7. . P. Ravi, J. Howe, A. Chattopadhyay, and S. Bhasin, ACM Computing Surveys. **54** (1), 1–39 (2021).
8. A. Shamir, Communications of the Association for Computing Machinery. **22** (11), 612–613 (1995).
9. A. Srinvasan and P. N. Vasudevan, in: *Advances in Cryptology — CRYPTO' 2019. Lecture Notes in Computer Science*, Vol. 11693 (Springer, Berlin, 2019), pp. 480–509.
10. N. P. Smart, *Cryptography Made Simple* (Springer International Publishing Switzerland, 2016).

A. Likhachov, B. Oliynyk

SECRET SHARING SCHEME BASED ON THE GOLDWASSER-GOLDRICH-HALEVI CRYPTOSYSTEM

With the development of quantum technologies, the issue of research and implementation of cryptographic primitives based on complex problems for quantum computing becomes relevant. Such cryptographic primitives are resistant to quantum cryptanalysis. Examples of problems with exponential complexity for quantum computing is lattice problems such as finding the shortest vector or finding the closest vector. One of the first and most famous quantum-resistant cryptosystems that use lattice problems as the basis of its mathematical apparatus is the Goldwasser-Goldrich-Halevi cryptosystem.

A secret distribution scheme is a fundamental cryptographic primitive that allows the distribution of a secret among a set of participants while the secret recovery is possible only when all or a certain part of the participants (the threshold of participants) is authorized. Also, a necessary condition for a secret distribution scheme is the impossibility of individual participants, or groups of participants whose number is less than the threshold, to recover the secret. Variants of constructing secret sharing schemes on various mathematical models, including lattices, are currently being actively studied since they allow for security multiparty calculations and secure information dissemination by distributing the original data between different servers. It is also used for constructing compilers of schemes with protection against leakage, etc. In this paper, a new quantum-stable n-threshold secret sharing scheme for n participants, based on the Goldwasser-Goldrich-Halevi cryptosystem, is proposed.

Keywords: integer lattice, Babai algorithm, Goldwasser-Goldrich-Halevi cryptosystem, secret sharing scheme, asymmetric encryption algorithm.

Матеріал надійшов 07.01.2025