станів багатоканальної моделі M/M/s. У випадку, коли число заявок в черзі більше, ніж на сервері контролера, обробка буде відбуватися з тією ж частотою μ, при цьому контролер буде гранично заповнений (рис.1).

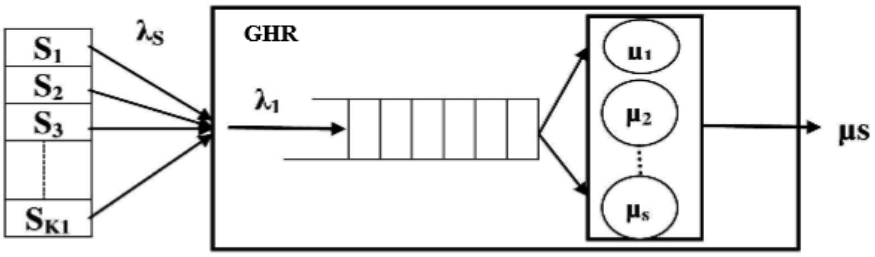


Рис. 1 – Представлення процесу дозволу ідентифікаторів на сервері GHR у вигляді об'єктів ЗМО

Частота отримання заявок λ_j реєстру GHR Gj розраховується як сума середніх частот отримання заявок на локальних реєстрах (L_i^j), приєднаних до реєстру G_j :

$$\lambda_j = \sum_{Li} \lambda_l. \quad (4)$$

Середнє навантаження на сервер-посередник G_j розраховується як середнє число отриманих і оброблених запитів. За допомогою формули Ерланга розраховується середнє навантаження L_j на реєстрах GHR:

$$L_j(\lambda) = s\gamma + \frac{\gamma}{1-\gamma} f\left(s, \frac{\lambda_j}{\mu}\right). \quad (5)$$

Таким чином, на основі отриманої формули Ерланга можна провести чисельний розрахунок середнього навантаження Lj на реєстрах GHR.

Список посилань

1. Recommendation ITU-T Y.2060 SERIES Y: Provides an overview of the Internet of things (IoT) (06/2012). 2. Internet of Things World Forum, IWF (https://www.iotwf.com/)
2. Інтернет ресурс: https://azure.microsoft.com/ru-ru/solutions/iot/iot-technology-protocols/.
3. Інтернет ресурс: https://habr.com/ru/post/299910/.

УДК 004.056

Розломій І.О., канд. техн. наук, ст. викладач
Воєводін Є.В., аспірант
Черкаський національний університет імені Богдана Хмельницького, inna-roz@ukr.net

ПРОБЛЕМА РЕТРОСПЕКТИВНОГО ДЕКОДУВАННЯ ДАНИХ: ОГЛЯД МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ КВАНТОВИХ ТЕХНОЛОГІЙ

Сучасні системи захисту інформації побудовані з використанням алгоритмів симетричного та асиметричного шифрування, таких як RSA чи то AES. Скажімо, TLS протокол, який використовується для безпечного обміну даних в мережі інтернет і не тільки, використовує асиметричне кодування для обміну секретним ключем, що дає змогу використати секретний ключ для подальшого симетричного кодування безпосередніх даних. Тобто має місце комбінація асиметричного та симетричного шифрування, що дозволяє досягти ефективного та безпечного обміну даними.

Перспектива розвитку науки та інформаційних технологій ставить під ризик надійність сучасних методів шифрування, так, маючи достатньо потужний квантовий комп'ютер, можна вирішити задачу факторизації та декодувати закодовані дані, використовуючи алгоритм Шора [1]. Це ставить під загрозу не тільки шифрування даних в майбутньому, але

й зашифровані дані, якими обмінюються в сучасних системах. Скажімо, зловмисник зберігає закодовану інформацію уже зараз, прослуховуючи зашифрований канал комунікації, без змоги цю інформацію декодувати на даний момент. Але в майбутньому, якщо така змога з'явиться, зловмисник зможе декодувати уже збережені дані. В загальному випадку, такий підхід називається – «ретроспективне декодування», або ж «зберігай зараз, декодуй потім» [2]. Можливість ретроспективного декодування робить дослідження методів та засобів захисту інформації як ніколи актуальною темою.

Як виявляється квантові технології також з користю використати для захисту інформації. До відомих методів захисту інформації на базі квантових технологій можна віднести [3]:

1. Квантовий ключовий обмін. Цей метод використовує фізичні закони квантової механіки для створення криптографічного ключа, який може буде безпечно поділений між двома сторонами. Основний протоко для квантового ключового обміну, відомий як квантовий обмін ключами Беннета-Брассара, або BB84, використовує передачу квантових бітів через незахищений канал зв'язку, під час якої будь-яке перехоплення буде помічено.

2. Квантовий прямий безпечний зв'язок. Метод, який використовує квантові властивості для безпечного обміну інформацією між сторонами. Він забезпечує конфіденційність, цілісність та автентичність даних, дозволяючи передачу квантових станів через квантовий канал. Квантові стани використовуються для безпечної комунікації між відправником і одержувачем, уникаючи необхідність безпосереднього кодування даних.

3. Квантову аутентифікацію. Метод, який використовує квантові системи для перевірки автентичності користувачів і пристроїв. Один з протоколів – Quantum Fingerprinting Protocol (QFP). QFP використовує квантові стани для ідентифікації і аутентифікації користувачів на основі їх унікальних квантових відбитків. Quantum One-Time Passwords (QOTP) [4] – є іншим протоколом квантової аутентифікації. Даний протокол використовує квантові стани для генерації одноразових паролів, які змінюються з кожним вимірюванням. Користувачі отримують випадкові квантові стани, які вони вимірюють та надсилають до сервера в якості одноразового пароля. Сервер перевіряє отриманий пароль, виконуючи аналогічне вимірювання. QOTP забезпечує високий рівень надійності та захисту від підробки паролів, оскільки кожен пароль є унікальним та не може бути використаний повторно.

4. Квантовий цифровий підпис. Метод, який використовує властивості квантових систем для створення підписів, що гарантують автентичність та незмінність даних. Основна перевага квантового цифрового підпису полягає в тому, що будь-яка спроба модифікації підписаного повідомлення буде помічена. Це робить квантовий підпис ефективним засобом для забезпечення автентичності повідомлень.

5. Квантове розділення секрету. Метод, який використовує квантові властивості для розподілу секретної інформації між декількома учасниками таким чином, що жоден із них самостійно не може отримати повну інформацію про секрет, але спільні зусилля учасників дозволяють відновити секрет в оригінальній формі. Метод включає кроки генерації початкового секрету, його кодування з використанням квантових станів, розділення кодованих станів між учасниками, збирання секрету на основі частин учасників та перевірку його цілісності.

Узагальнюючи, проблема ретроспективного декодування даних підвищує актуальність дослідження альтернативних методів шифрування. Галузь квантової криптографії описує широкий спектр методів, які можна використати для вирішення проблеми ретроспективного декодування, застосовуючи криптографічні протоколи на базі квантових технологій.

Список посилань

1. Mandl, A. (2021). Quantum Algorithms for the Discrete Logarithm Problem. Masters thesis, TU Wien.

2. Townsend K. Solving the Quantum Decryption ‘Harvest Now, Decrypt Later’ Problem. URL: https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/ (дата звернення: 19.05.2023).

3. Korchenko O., Vasiliu Y., Gnatyuk S. Modern quantum technologies of information security against cyber-terrorist attacks. Aviation. 2010. T. 14, № 2. C. 58–69.

4. Sharma, M. K., & Nene, M. J. (2020). Quantum one time password with biometrics. In Innovative Data Communication Technologies and Application: ICIDCA 2019 (pp. 312-318). Springer International Publishing.

УДК 612:656.7.086.1 (044)

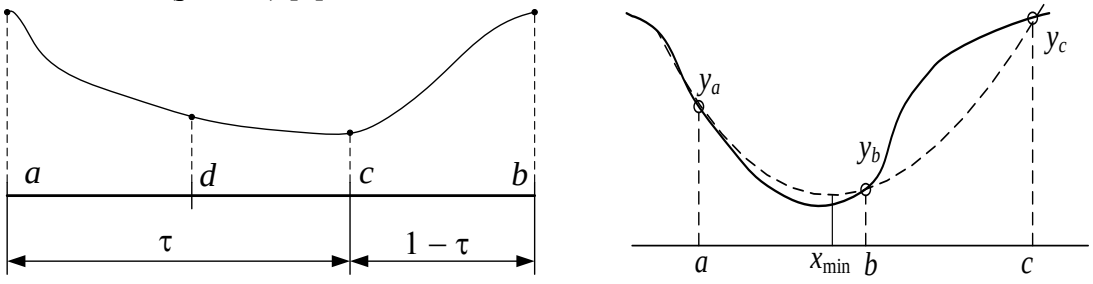
Бориченко М.Ю., канд. техн. наук, доцент
Іванець О.Б., канд. техн. наук, доцент
Архирей М.В.
Корчемний М.С., студент
Шевченко Т.Р., студентка
Національний авіаційний університет, м. Київ, olchik2104@ukr.net

ОПТИМІЗАЦІЯ ФУНКЦІЙ НА ОСНОВІ МЕТОДІВ ВСТАНОВЛЕННЯ ІНТЕРВАЛІВ НЕВИЗНАЧЕНОСТІ

Складнощі аналізу складних об’єктів полягає в наявності джерел невизначеності первинної інформації про параметри даних об’єктів [1,2]. Для побудови алгоритмів одновимірної оптимізації цільової функції використовують методи встановлення інтервалу невизначеності [3].

В роботі проаналізоване використання наступних методів оптимізації для зменшення інтервалів невизначеності при аналізі складних об’єктів різної природи: метод золотого перерізу, метод параболічної інтерполяції, метод Брента [4].

Метод золотого перерізу, що полягає у використанні золотого перерізу відрізка за рахунок ділення відрізка на дві частини, при якому відношення довжини всього відрізка до довжини більшої частини дорівнює відношенню довжини більшої частини до довжині меншої частини (рис. 1а) [3].



а) б)

Рис. 1 – Графічне представлення методів оптимізації: а)метод золотого перерізу, б) метод параболічної інтерполяції

Після кожній ітерації алгоритму довжина поточного інтервалу невизначеності $L = b – a$ скорочується в τ разів. Кількість ітерацій K, необхідних для знаходження мінімуму функції $f(x)$ з точністю ε, можна оцінити з умови $(b – a)\tau^K \le \varepsilon$.

Метод параболічної інтерполяції застосовує поліном низького порядку $P(x)$ для апроксимації цільової функції на інтервалі пошуку, а потім використовують точку мінімуму полінома апроксимації P(x) як точку ділення нового інтервалу, причому якщо функція поблизу мінімуму близька до параболічної, то парабола проведена через три точки цієї функції може одним кроком привести до мінімуму, або дуже близько до нього.