4. Swarm mode overview // Documentation : [website]. Palo Alto, California : Docker : Docs, 2023. URL: https://docs.docker.com/engine/swarm/.
5. MySQL Cluster CGE // Documentation : [website]. Santa Clara, California : MySQL : Products, 2023. URL: https://www.mysql.com/products/cluster/.

УДК 621.372

МОЛЕКУЛЯРНА КРИПТОГРАФІЯ В КІБЕРБІОБЕЗПЕЦІ

Марія-Ольга Пішковцій [1], Василь Різак[2]
Ужгородський національний університет,
[1]mariia-olha.pishkovtsii@uzhnu.edu.ua, [2]vrizak@uzhnu.edu.ua

Експоненційний ріст світових біонаук та біоекономіки за останні 20 років призвів до прогресу в молекулярній біології, включаючи синтетичну біологію та біотехнологію, а також значні інновації в медицині, охороні здоров'я, енергетиці та обороні. Проте державний та приватний сектори повинні об'єднатися, уможливити подальші законні та міждисциплінарні дослідження та розробки в широкій галузі біології та біоекономіки, також пам'ятаючи про аспекти безпеки, пов'язані з такою діяльністю. Використання перетину таких явищ як цифрові технології та біологія дає значні переваги для здоров'я, економіки та національної безпеки, але також може призвести до збільшення ризиків і вразливості. Досягнення в науці вершин (особливо розробка нових ШІ-технологій і алгоритмів для аналізу та візуалізації даних і розпізнавання нових функцій) і використання біоінженерії для маніпулювання або створення нових біологічних організмів, які мають конкретні нові функції, змінюють здоров'я, енергію, виробництво та екологічні сектори.

Кібербіобезпека є відносно новою сферою, яка прагне захистити цифрові біологічні та медичні дані, щоб захистити індивідуальну, громадську, інфраструктуру охорони здоров'я та розвиток біотехнологічних інновацій. З розвитком технологій та інтернету кіберзагрози стають все більш складними та небезпечними. Одним із способів протидіяти таким загрозам є використання ДНК - молекули, що містить генетичний код живих організмів.

Молекулярна криптографія - це напрям криптографії, що використовує молекули або живий організм, як носії або засоби обчислень для шифрування та дешифрування інформації. Ця галузь може вирішити деякі проблеми традиційних методів, але також створює нові виклики та питання, пов'язані з надійністю, доступністю, стандартизацією та етикою.

Молекулярна криптографія має декілька переваг перед традиційними методами, такими як: висока щільність збереження даних, висока стабільність даних, висока складність атак. Також її можна застосувати, як: 1) створення молекулярних шифрів - це методи шифрування, що використовують молекули як ключі або носії інформації. Наприклад, можна використовувати ДНК-синтез для кодування повідомлень у послідовностях нуклеотидів або використовувати хемосигнали для передачі таємних сигналів. 2) розробка молекулярних протоколів

- це способи взаємодії між молекулярними системами для досягнення певних криптографічних цілей. Наприклад, можна використовувати молекулярну імітацію для моделювання складних криптографічних алгоритмів або використовувати молекулярну комутацію для перемикання станів шифру. 3) застосування молекулярної біометрії - це використання молекулярних особливостей для ідентифікації та верифікації особистостей. Наприклад, можна використовувати ДНК-профайл або антитіла для розпізнавання особи або використовувати ензими або рецептори для перевірки певних ознак.

ДНК - це довгий полімер, що складається з двох ланцюгів нуклеотидів, які утворюють подвійну спіраль. Кожен нуклеотид містить одну з чотирьох азотистих основ: аденін, тимін, гуанін або цитозин. Послідовність нуклеотидів визначає генетичну інформацію, яка кодує будову та функції білків. ДНК можна розглядати як носій інформації, що має високу щільність (один грам ДНК може зберегти до 215 Петабайт даних), стабільність (ДНК може зберігатися протягом тисячоліть) та унікальність (ДНК кожної людини має варіабельні тандемні повтори (ВТП), що роблять її ідентифікатором).

ДНК-криптографія - це використання ДНК як носія інформації та обчислень для шифрування та дешифрування. ДНК-криптографія може застосовувати різні методи, такі як ДНК-шифрування, ДНК-стеганографія, ДНК-комп'ютери, ДНК-безпека та ДНК-збереження. ДНК-шифрування - це метод перетворення текстової або бінарної інформації на послідовності ДНК за допомогою певного алгоритму. Наприклад, можна використовувати простий правило: A = 00, T = 01, G = 10, C = 11. Таким чином, слово "кріп" можна зашифрувати як ДНК-послідовність "TGTAAGGA". Щоб отримати дешифроване повідомлення, потребується знати ключ - місце початку та кінця прихованого тексту. Перевагами є непомітність даних, можливість використання живих організмів як носіїв інформації та стійкість до знищення. Використання генетичного шифрування має великий потенціал розвитку в споріднених наука до кібербіобезпеки, об'єднуючи в собі десятки наук, наприклад, біологію, фізику, математику, інформатику, криптографію, кібербезпеку, менеджмент, правознавство. Але як кожне рішення, створює ще більше питань, тому потрібно до цієї теми підходити із викликом. Деякі з них є: - синтез та маніпуляція молекул - це процеси, що вимагають високої точності, складності та витрат. Необхідно розробляти нові методи та інструменти для створення та контролю молекулярних структур та процесів, що можуть служити як надійні криптографічні примітиви; - аналіз та перевірка молекулярних протоколів - це завдання, що потребують глибокого розуміння молекулярної динаміки, хемосигналінгу та інших феноменів, що впливають на поведінку молекулярних систем. Необхідно розробляти нові математичні моделі та методи для оцінки безпеки та ефективності молекулярних протоколів у реальних умовах; - сумісність та інтеграція з класичною криптографією - це вимога, що ставиться перед молекулярною криптографією, щоб вона могла співпрацювати з існуючими криптографічними стандартами та системами. Необхідно розробляти нові схеми та алгоритми для перетворення молекулярної інформації в класичну та навпаки, а також для гармонізації молекулярних та класичних ключів, підписів, хеш-функцій.

Це лише деякі з покликів, які стоять перед молекулярною криптографією. Ця галузь науки ще знаходиться на початковому етапі розвитку і потребує багато

досліджень і експериментів для досягнення свого потенціалу. Але цей метод однозначно має переваги порівняно з класичною криптографією, такі як: висока стійкість до квантових атак - молекулярні шифри не базуються на математичних задачах, які можуть бути ефективно розв'язані квантовими алгоритмами, а на фізичних властивостях молекул; велика розмаїтість та гнучкість молекулярних примітивів - молекулярна криптографія може використовувати різні типи молекул та хемосигналів для реалізації різних криптографічних функцій, таких як шифрування, хешування, псевдовипадкова генерація тощо; низька вартість та енергоспоживання - молекулярна криптографія не потребує складного обладнання та високої потужності для своєї роботи, можуть працювати за допомогою хімічних реакцій та дифузії, що забезпечують низьку вартість та енергоспоживання. Це лише деякі з переваг молекулярної криптографії. Ця галузь науки відкриває нові можливості для захисту інформації в різних сферах, особливо в біомедицині та нанотехнологій. може пропонувати нові методи для захисту інформації в умовах зростаючих загроз з боку квантових комп'ютерів та байотехнологій.

Молекулярна криптографія має переваги порівняно з класичною криптографією, такі як: - висока стійкість до квантових атак - молекулярні шифри не базуються на математичних задачах, які можуть бути ефективно розв'язані квантовими алгоритмами, а на фізичних властивостях молекул. Тому вони можуть протистояти загрозам від квантових комп'ютерів; - велика розмаїтість та гнучкість молекулярних примітивів - молекулярна криптографія може використовувати різні типи молекул та хемосигналів для реалізації різних криптографічних функцій, таких як шифрування, хешування, псевдовипадкова генерація тощо. Також можливо створювати гібридні схеми, що поєднують молекулярну та класичну криптографію; - низька вартість та енергоспоживання - молекулярна криптографія не потребує складного обладнання та високої потужності для своєї роботи. Молекулярні системи можуть працювати за допомогою хімічних реакцій та дифузії, що забезпечують низьку вартість та енергоспоживання.

Отже, ця галузь науки є перспективною та інноваційною, оскільки вона поєднує фундаментальні знання з практичною користю. Молекулярна криптографія - це галузь криптографії, що використовує молекулярні структури та реакції для забезпечення безпеки інформації. Молекулярна криптографія може мати декілька переваг перед традиційними методами шифрування, такими як висока щільність зберігання даних, невидимість для звичайних детекторів, висока складність для криптоаналізу та можливість самознищення. Молекулярна криптографія також ставить нові виклики для науковців та інженерів, які повинні розробляти ефективні способи синтезу, кодування, передачі, зчитування та розшифрування молекулярних повідомлень. Цей метод має потенціал стати майбутньою технологією для захисту даних від несанкціонованого доступу та злому. Однак молекулярна криптографія також потребує подальших досліджень та розвитку для досягнення практичної застосовності та надійності.

Науковий керівник – доктор фіз.-мат. наук, професор, Різак В.М.