МОДЕЛЮВАННЯ ХЕШ-ФУНКЦІЙ НА ОСНОВІ НЕЗВІДНИХ ПОЛІНОМІВ

Булина Ярослав Віталійович
аспірант факультету інформаційних технологій
ДВНЗ «Ужгородський національний університет», м. Ужгород, Україна

У зв'язку зі стрімким розвитком інформаційних технологій та зростанням обсягів обробки даних, безпека та ефективність хеш-функцій стають важливими аспектами в галузі криптографії та інформаційної безпеки [1]. Однак з інтенсивним зростанням обсягів даних виникають проблеми стійкості та продуктивності існуючих хеш-функцій, що вимагає дослідження нових підходів до їх розробки. Важливо враховувати, що ефективні хеш-функції не тільки забезпечують безпеку, але і забезпечують оптимальну продуктивність обчислень.

Останнім часом, у контексті розробки хеш-функцій, спостерігається великий інтерес до використання теорії кінцевих полів та незвідних многочленів. Ці теоретичні концепції вже успішно використовуються в криптографії, а їхнє застосування в галузі хеш-функцій може виявитися ефективним для подолання майбутніх викликів у сфері інформаційної безпеки.

Хеш-функція – це математичний алгоритм, який приймає вхідні дані і видає результат фіксованого розміру, відомий як хеш-значення або хеш-код. Ці хеш-значення є унікальними і, по суті, діють як цифрові відбитки пальців для вхідних даних. Будь-яка незначна зміна у вхідних даних призведе до абсолютно іншого хеш-значення, що робить їх життєво важливими для перевірки цілісності даних і захисту паролів.

Одним з підходів до створення хеш-функцій є використання незвідних поліномів у скінченних полях. Скінченні поля, також відомі як поля Галуа [2], є алгебраїчними структурами, які містять скінченну кількість елементів. Їх часто представляють у вигляді GF(p^n), де p - просте число, а n - натуральне число. Однією з ключових властивостей скінченних полів є те, що вони володіють характеристикою, яка визначає порядок поля. Арифметичні операції в скінченних полях виконуються за особливими правилами, які відрізняються від правил традиційної арифметики. Ці унікальні властивості роблять скінченні поля ідеальною основою для реалізації криптографічних алгоритмів.

Над цими скінченними полями визначаються незвідні поліноми, які слугують будівельними блоками для побудови хеш-функцій. При використанні в якості основи для моделювання хеш-функцій, незвідні поліноми дають кілька переваг. По-перше, використання незвідних поліномів забезпечує рівномірний розподіл хеш-значень. Іншими словами, різні вхідні дані даватимуть хеш-значення, які важко корелювати. Ця властивість є важливою для запобігання колізій і підтримки безпеки хеш-функції. Колізії виникають, коли два різні вхідні дані створюють однакове хеш-значення, що ставить під загрозу цілісність і автентичність даних. По-друге, незвідні поліноми дозволяють ефективно обчислювати хеш-значення. Використовуючи математичні властивості скінченних полів, процес обчислення хеш-значення можна оптимізувати. Це особливо важливо для обчислювально інтенсивних задач [3], таких як хешування великих обсягів даних або робота з пристроями з обмеженими ресурсами [4]. Крім того, вибір незвідних поліномів впливає на криптографічну стійкість хеш-функції. Складність обернення хеш-функції та виявлення початкового вхідного сигналу (так

званого першовзору) залежить від властивостей незвідного полінома, що лежить в її основі. Вибираючи відповідний поліном, можна підвищити криптографічну стійкість хеш-функції.

Моделювання хеш-функцій на основі незвідних поліномів складається з декількох кроків. По-перше, з набору заздалегідь визначених поліномів вибирається відповідний незвідний поліном. Вибір полінома залежить від різних факторів, включаючи бажаний рівень безпеки, довжину хеш-значення та обчислювальну складність. Після того, як поліном обрано, він використовується для побудови поля Галуа, яке є основою для подальших операцій. Наступний крок полягає у визначенні внутрішнього перетворення хеш-функції. Це перетворення використовує незвідний поліном для виконання побітових операцій над вхідними даними, ефективно створюючи унікальне хеш-значення для кожного входу. Конкретні операції залежать від обраного полінома і бажаного рівня складності. Загальні операції включають XOR, зсув і підстановку, які застосовуються ітеративно до кожного блоку або елементу вхідних даних. Останнім кроком у моделюванні хеш-функцій на основі незвідних поліномів є розробка відповідної архітектури хеш-функції. Ця архітектура визначає загальну структуру, потік даних і обчислювальну ефективність хеш-функції. Кілька популярних архітектур, таких як архітектура Меркле-Дамгарда, були успішно адаптовані для включення незвідних поліномів для підвищення безпеки.

Однією з ключових переваг моделювання хеш-функцій на основі незвідних поліномів у скінченних полях є властивий їм паралелізм обчислень. Оскільки поліноми складаються з коефіцієнтів, які можуть оброблятися незалежно, великомасштабні обчислення можуть бути ефективно розподілені між декількома процесорами або системами, що призводить до прискорення обчислень хеш-функцій. Це робить такі хеш-функції придатними для додатків, які вимагають високопродуктивних обчислень, таких як хмарні сховища даних або розподілені системи [5]. Широко використовуються хеш-функції також в задачах на олімпіадах різного рівня [6] та турнірах юних інформатиків [7].

Висновки. Математична складність та висока стійкість до атак, особливо тих, що базуються на аналізі структури многочленів, роблять ці алгоритми важливим інструментом для забезпечення цілісності та конфіденційності даних. Незвідні многочлени, як ключовий елемент конструкції, додають до хеш-функцій непередбачуваність, що робить їх ефективними для застосувань, де важлива надійність захисту інформації. Однак важливо враховувати, що висока обчислювальна складність може впливати на швидкодію алгоритмів, що може бути важливим фактором у великих обчислювальних завданнях. Звідси виникає потреба в обдуманому виборі алгоритму, залежно від конкретних потреб та обмежень в конкретному використанні.

Список використаних джерел:

1. M. O. Rabin, R. M. Karp. Efficient randomized pattern-matching algorithms, IBM, 1987, pp. 249 – 260.
2. R. Lidl, H. Niederreiter. Finite Fields, 1997, pp. 768.
3. Міца О.В., Булина Я.В. Розробка програмного забезпечення для перевірки даних великої розмірності на відповідність певним законам. The 10th International scientific and practical conference “Results of modern scientific research and development” (December 12-14, 2021). Barca Academy Publishing, Madrid, Spain. С. 200-205.
4. Mulesa O., Mitsa O., Geche, F., Dulo V., Radivilova T. Development of the group problem solving method in designing traffic flows. 2022 International Conference on Smart Information Systems

and Technologies «SIST 2022»: conference proceedings (Nur-Sultan, Kazakhstan, 28-30 April 2022). Nur-Sultan, 2022. P. 451-455.
5. Mitsa, O., Sharkan, V., Maksymchuk, V., Varha, S., & Shkurko, H. (2023). Ethnocultural, Educational and Scientific Potential of the Interactive Dialects Map. In 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST) (pp. 226-231). Astana, Kazakhstan. doi: 10.1109/SIST58284.2023.10223544.
6. Мельник В.І., Горошко Ю.В., Міца О.В. Огляд систем підготовки до олімпіад з інформатики в деяких країнах. II Всеукраїнської науково-практичної конференції з міжнародною участю «Сучасні інформаційні технології в освіті і науці». Житомир. 2017. С.21-23.
7. Горошко Ю.В., Мельник В.І., Міца О.В. Про турніри юних інформатиків. Комп'ютер у школі та сім'ї: Науково-методичний журнал. 2017. N 8. С. 17-24.