АЛГОРИТМ ХЕШ-ФУНКЦІЇ З ПІДВИЩЕНОЮ КРИПТОСТІЙКІСТЮ. ПОКРАЩЕННЯ ЛАВИННОГО ЕФЕКТУ

Дячук Р.Л., Добровольський Ю.Г.

Чернівецький національний університет імені Юрія Федьковича, м. Чернівці

Для безпеки передачі потоків даних часто використовуються криптографічні хеш-функції. Хеш-функції використовуються в сучасній криптографії для різноманітних цілей, зокрема для порівняння наборів даних, пошуку збігів у наборах, тощо. З метою вирішення нових питань у сфері інженерії програмного забезпечення це дослідження спрямоване на визначення найкращого компромісу між перевагами та недоліками існуючих алгоритмів хешування.

Багато рішень, натхненних блокчейном, покладаються на оригінальні алгоритми SHA-2 і SHA-3 та їх варіації для своєї надійності. Вони детально висвітлені в [1], де були ретельно вивчені як їхні переваги, так і недоліки.

Однією зі складових криптографічної міцності хеш-функцій є чутливість до лавинного ефекту. Це підвищення чутливості до змін в хеші, що ускладнює отримання незашифрованих даних. Як видно з [3], збільшення кількості ітерацій під час кроку перетворення дозволило досягти максимального значення чутливості. Однак таке зростання вимагає додаткової обчислювальної потужності. Ми надаємо наступне, щоб посилити алгоритм, обмеживши використання ресурсів комп'ютера. Спочатку виконується створення ініціалізаційного блоку. Для генерації використовується клітинний автомат. Відкритий текст циклічно стискається в блоки. Отже, ми отримуємо хеш, стиснутий до 128 біт. Потім використовується функція перетворення. Запропонована хеш-функція повинна мати мінімальну чутливість до лавинного ефекту, що має значно підвищити її надійність.

У розробленому алгоритмі є псевдохаотична залежність вихідного байту від вхідного. Ця залежність встановлюється за допомогою клітинних автоматів хаотичного класу. За допомогою великої кількості ітерацій, можливо досягти максимальної незалежності між бітами. Для цього в нашому алгоритмі було використано 256 ітерацій, що ще більше заплутує вихідне повідомлення. Проте також це суттєво впливає на швидкодію алгоритму.

Саме тому згідно з метою нашого дослідження, ми пропонуємо новий метод, згідно з яким можна знайти баланс між швидкодією та стійкістю до лавинного ефекту.

Література:

1. Kuznetsov A.A. Research of cryptographic hashing algorithms used in modern blockchain systems / A.A. Kuznetsov, Yu.I. Gorbenko,V.V. Onoprienko, I.V. Stelnik, D.V. Myalkovsky // Radio engineering. 2019. Issue. 198. -c. 154-174. https://doi.org/10.30837/rt.2019.3.198.05

2. Dobrovolsky Y. Development of a hash algorithm based on cellular automata and chaos theory / Y. Dobrovolsky, D. Hanzhelo, M. Hanzhelo, D. Trembach, G. Prokhorov // Eastern-European Journal of Enterprise Technologies. 5/9 (113) 2021. P. 48-55. DOI: 10.15587/1729-4061.2021.242849.