Гедеон Г. О., магістрантка,
спеціальність «Комп'ютерна інженерія»,
Гапак О. М., доцент кафедри комп'ютерних систем та мереж
Ужгородський національний університет

АПАРАТНА РЕАЛІЗАЦІЯ МОДУЛІВ ХЕШУВАННЯ НА БАЗІ АЛГОРИТМІВ CRC-32 І ADLER-32

У сучасному суспільстві інформація стає найбільш важливою цінністю, а індустрія отримання, обробки і захисту інформації – провідною галуззю діяльності, куди з кожним роком вкладають все більш значні капітали. Вже найближчим часом саме розвиток інформаційної сфери, рівень інформаційної безпеки будуть визначати політичну й економічну роль окремих держав на світовій арені. Для досягнення оптимальної швидкодії та надійності захисту інформації раціонально використовувати не лише програмні продукти, а й апаратні розробки для шифрування та хешування. Саме вони гарантують цілісність розробки та виключають можливість перехоплення інформації. Метою роботи є розробка апаратного модуля хешування на базі алгоритмів CRC-32 і Adler-32, що дозволяє в подальшому доповнювати новими алгоритмами, за короткий час знаходити хеш-суми для паролів і кодів доступу та забезпечувати надійність передачі даних незахищеними каналами. Апаратний модуль, що включає декілька алгоритмів хешування, може використовуватись в якості окремої мікросхеми, що під'єднується до каналу зв'язку, або як окремий пристрій для миттєвого відображення контрольної суми для введеного вхідного повідомлення. Для реалізації модуля обрано засіб розроби і проектування електронних пристроїв Multisim – National Instruments. В якості алгоритмів хешування загального призначення обрано алгоритм CRC-32 (обчислює 32-бітний хеш) та алгоритм Adler-32 (знаходить хеш-суму аналогічного розміру).
Алгоритм CRC-32:

1. На регістр зберігання даних поступає вхідне слово, яке перетворюється в послідовність одиниць та нулів.
2. Блок хешування аналізує кожен біт, що поступає в відповідний регістр, та виконує обчислення з заданим поліномом.
3. Лічильник контролює функціонування блоку хешування та в разі необхідності подає сигнал дозволу на запис регістру хешу.
4. Після подання сигналу обчислення блоком хешування припиняються та регістр хешу демонструє результати – контрольну суму.

Алгоритм Adler-32:

1. На регістр зберігання даних поступає вхідне слово, яке перетворюється в послідовність одиниць та нулів.
2. Блок хешування зчитує посимвольно вхідне слово та розділяє кожен символ (послідовність 1 та 0) на частини A та B. Кожна частина надсилається на відповідний блок для проведення обрахунків.
3. Лічильник контролює функціонування блоку хешування та в разі необхідності подає сигнал дозволу на перевірку розміру хешу.
4. Блок хешування формує хеш з отриманих частин A та B та перевіряє, чи не перевищений ліміт.
5. Блок керування передає сигнал дозволу на демонстрацію отриманої контрольної суми.

Виконано схематичне представлення апаратного хеш-модуля, реалізовано функціональні блоки, в тому числі блоки керування, блоки індикації, які необхідні для роботи обраних алгоритмів. Змоделювано роботу схеми. Проведено аналіз швидкодії та зроблена оцінка ефективності роботи апаратного модуля в порівнянні з програмною реалізацією алгоритмів. При використанні апаратного модуля хешування значно підвищується надійність передавання даних незахищеними каналами, виключається можливість підбору паролів чи кодів доступу та забезпечується можливість вибору бажаного алгоритму з запропонованих (швидкодія та логіка виконання алгоритмів дещо відрізняється).

Апаратна реалізація алгоритмів загального призначення гарантує цілісність розробки: після змінення деяких параметрів пристрою, блок повністю виходить з ладу, адже будь-які зміни впливають на результати обчислень та не дозволяють підібрати вхідне слово. Відсутність підпрограм компенсується блоками управління на базі автоматів Мура, які також підвищують швидкодію та надійність апаратного модулю.

Список використаних джерел

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко, Л. В. Бурячок, П. М. Складанний, Н. В. Лукова-Чуйко. – Київ: ДУТ – КНУ, 2016.
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. – Харків: Форт, 2013.
3. Гулак Г. М. Основи криптографічного захисту інформації: підручник / Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук.– Вінниця: ВНТУ, 2011.