УДК 004.4

В. І. Селезньов

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ВІДДАЛЕНОГО СТАТИСТИЧНОГО ТЕСТУВАННЯ МЕТОДІВ МАЛОРЕСУРСНОГО ГЕШУВАННЯ ЗА ДОПОМОГОЮ ПАКЕТУ NIST STS 822

Вінницький національний технічний університет

Анотація

Проаналізовано проблематику тестування та перевірки безпеки нових методів криптографічного гешування. Розглянуто методику тестування криптографічних засобів NIST STS. Представлено програмний засіб для здійснення тестування криптографічних геш-функцій за з використанням тестів NIST STS на віддаленому сервері.

Ключові слова: програмний засіб, малоресурсна криптографія, гешування, псевдовипадкова послідовність, статистичне тестування.

Abstract

The issues of testing and verifying the security of new cryptographic hashing methods are analyzed. The testing methodology of cryptographic tools using NIST STS is discussed. A software tool for conducting cryptographic hash function testing using NIST STS tests on a remote server is presented.

Keywords: software application, lightweight cryptography, hashing, pseudorandom sequence, statistical testing.

Вступ

В сучасному світі безпека даних та конфіденційність інформації відіграють важливу роль у багатьох сферах діяльності. Одним з ключових аспектів захисту інформації є забезпечення високого рівня криптографічного захисту, зокрема за допомогою геш-функцій. З появою все більшої кількості малоресурсних пристроїв постає необхідність у вдосконаленні або розробці нових методів малоресурсного гешування, при чому постає постійна проблема перевірки надійності запропонованих методів. Для досягнення безпеки необхідно, щоб малоресурсна геш-функція забезпечувала:

- стійкість до колізій: два різні набори даних повинні мати різні результати перетворення, тобто для заданого повідомлення M повинно бути практично неможливо підібрати інше повідомлення M', для яких буде однаковим результат гешування;
- безповоротність (неможливість обчислити початкові дані по результату перетворення);
- наявність лавинного ефекту (будь-які, навіть незначні, зміни у повідомленні M призводять до значних змін у геш-значенні) [1].

Послідовність, сформована з геш-значень повинна бути псевдовипадковою, інакше, для цього перетворення не буде забезпечено стійкість до колізій.

Існують спеціальні методики тестування для оцінки якості випадкових послідовностей. Для дослідження якості псевдовипадкових послідовностей використовують статистичні тести. Статистичні тести використовуються для перевірки певної нульової гіпотези H_0 щодо випадковості сформованої послідовності. З цією нульовою гіпотезою пов'язана альтернативна гіпотеза H_a про те, що послідовність не випадкова. Серед найрозповсюдженіших методів статистичного тестування тести Дональда Кнута, система статистичного тестування DIEHARD, методика FIPS, методика AIS, а також методика NIST STS [2, 3, 4].

Результати розробки

Статистичні тести NIST забезпечують перевірку послідовності біт на випадковість. Для кожного тесту отримують висновок про прийняття або відхилення нульової гіпотези, ґрунтуючись на сформованій досліджуваним генератором послідовності. Кожен тест заснований на обчисленні значення тестової статистики, яка є функцією даних. Ця статистика використовує обчисленні значення P-value, за допомогою якого і визначається чи дана послідовність є випадковою. Для тесту обирається рівень значущості α . Якщо значення P-value $\geq \alpha$, то приймається нульова гіпотеза H_0, тобто послідовність є випадковою. Якщо значення P-value $< \alpha$, то нульова гіпотеза відхиляється, тобто послідовність не є випадковою. Як правило, значення α вибирається в інтервалі [0.001, 0.01] [2, 4].

До складу пакету NIST входять 15 статистичних тестів, метою яких є визначення міри випадковості двійкових послідовностей: частотний монобітний, частотний блоковий, тест перевірки серій, найдовшої серії з одиниць, перевірки рангу двійкових матриць, тест на основі дискретного перетворення Фур'є, тест на співпадіння з шаблоном без перекриття, тест шаблонів з перекриттям, універсальний тест Мауера, тест лінійної складності, тест серій, тест на основі апроксимації ентропії, тест накопичених сум, тест випадкових відхилень та тест випадкових відхилень [5].

Програмний засіб для статистичного тестування використовує увесь набір тестів NIST STS, що представлений у [4]. Комп'ютерна програма оформлена у вигляді клієнт-серверного застосунку, написаного мовою програмування Python. Процес виконання тестування проходить на віддаленому сервері, що дозволяє використовувати обчислювальні потужності сервера для прискорення процесу тестування. Для виконання тестування генерується великий масив геш-значень за допомогою обраного методу або модифікації малоресурсного гешування. Використання Python дозволяє динамічно додавати компоненти до програми. Подібним чином можна додати до програми модуль формату *.py з кодом методу гешування, що відповідатиме вказаному шаблону для здійснення його тестування. Взаємодія з серверною частиною та передача файлів здійснюється з використанням безпечних протоколів SSH та SFTP. Обсяг генерованих геш-значень та параметри тестування вказується перед початком виконання програми. За замовчуванням застосунок виконує тестування методу HDG, запропонованого авторами [6] та генерує 200000 геш-значень довжиною 256 біт для статистичного тестування.

Висновки

Розроблений програмний засіб дозволяє здійснити статистичне тестування методикою NIST STS методів малоресурсного гешування і є повністю готовим до використання. Застосунок також можна використовувати для тестування будь-яких генераторів псевдовипадкових послідовностей та геш-функцій, що будуть підключені до нього у вигляді окремих Python модулів, які відповідають запропонованому шаблону. Програмна має консольний інтерфейс, завантажує та групує результати для кожного окремого дослідження, дозволяє використовувати хмарні обчислювальні потужності для виконання обчислень при тестуванні. В подальшому застосунок можна покращити шляхом інтеграції з іншими системами статистичного тестування або шляхом додавання інших методик тестування геш-функцій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Володимир Лужецький, Юрій Баришев. Підхід до паралельного гешування даних на основі моделі кватерніона // Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф. – Львів : Видавництво Львівської політехніки, 2023. – С. 83-84

2. МЕТОДИКИ ТЕСТУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ URL: https://virt.ldubgd.edu.ua/pluginfile.php/14209/mod_folder/content/0/%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%20%D0%A3%D0%86%D0%91/%D0%9C%D0%B0%D0%BD%D0%B4%D1%80%D0%BE%D0%BD%D0%B0%20%D0%9C.%D0%9C/2012/12.pdf?forcedownload=1 (дата звернення 12.03.2024).

3. Мордвінов Р. І. Порівняльний аналіз методів та засобів тестування випадкових послідовностей nist 800-22 та nist 800-90b / Р. І. Мордвінов // Прикладна радіоелектроника : наук.-тех. журн. – Х. : ХНУРЕ, 2013. – Т. 12, № 2 – С. 250–253.

4. Rukhin A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology. 2010. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf (дата звернення 12.03.2024).

5. NIST 800-22 українською мовою URL: http://www.itsway.kiev.ua/pdf/Articles180106.pdf (дата звернення 13.03.2024).

6. Селезньов В. І., Лужецький В. А. Метод малоресурсного гешування типу «дані – генератор». Кібербезпека: освіта, наука, техніка. 2023. 2(22). С. 84-95.

Селезньов Віталій Ігорович — аспірант групи 125-22а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: seleznov.vitalii@gmail.com

Seleznov Vitalii — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: seleznov.vitalii@gmail.com