

РОЗРОБЛЕННЯ АРМ ДЛЯ НЕЗАЛЕЖНОЇ ВЕРИФІКАЦІЇ АЛГОРИТМІВ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Нейванов Андрій Вікторович
Харківський національний університет радіоелектроніки

В зв'язку з глобальною інформатизацією простору та використанням сучасних технологій обробки та передачі інформації виникла проблема захисту даних, що обробляються автоматизованими системами та передаються по швидкісним каналам зв'язку. Прикладом того є банківські системи "Клієнт-Банк", система платівок НС МЕР або будь-яка банківська локальна обчислювальна мережа в котрій циркулює інформація з обмеженим доступом та є необхідність використовувати IP шифратори.

Базові послуги захисту такі як конфіденційність та цілісність можуть забезпечуватись завдяки використанню алгоритмів блочних симетричних шифрів (БСШ). На даний час в Україні існує лише один стандартизований алгоритм БСШ, який дозволяє вирішувати задачі такого класу, це ГОСТ 28147-89. За рівнем стійкості до криптоаналітичних атак він відповідає рівню "задовільно" проекту NESSIE. Цей проект було створено в Європі з метою виявлення самого стійкого, надійного та швидкісного алгоритму БСШ котрий забезпечуватиме послуги конфіденційності та цілісності на сучасному рівні.

В 2006 році в Україні було оголошено конкурс на кращий перспективний БСШ. При розробці такого класу криптопримітивів необхідно вирішувати завдання, пов'язані з доведенням правильності реалізацій АРМів, виконаних різними розробниками. Особливістю нашої задачі є те, що верифікацію АРМів необхідно розробити для нового алгоритму. Для цього алгоритму не розроблено ні методик, ні АРМів реалізації.

В ході виконаної роботи трьом незалежним розробникам була поставлена задача розробити алгоритм БСШ за специфікацією з використанням алгоритмічної мови програмування "C++". На етапі завершення розробки АРМів нового БСШ усіма трьома розробниками виникла необхідність верифікації програмних модулів.

Програмні модулі відрізнялись за розміром на дисковому просторі, за об'ємом оперативної пам'яті, необхідної для завантаження процесу та його роботи. Також різною була швидкість роботи модулів. Результати досліджень можна побачити з Таблиці 1.

Таблиця 1 – Результати дослідження алгоритмів БСШ

	Дисковий простір	Об'єм необхідної оперативної пам'яті	Швидкість шифрування
Розробник №1	120Кб	712Кб	33.443557 Мб/сек.
Розробник №2	52Кб	572Кб	0.227030 Мб/сек.
Розробник №3	56Кб	656Кб	0.167281 Мб/сек.

Основним завданням, що вирішується на етапі розробок, було завдання узгодженості реалізацій за виконуваною специфікацією. Для вирішення проблеми такого класу були використані методики генерації тестових векторів, запропоновані для БСШ – кандидатів у проекті США на сучасний стандарт шифрування AES (Advanced Encryption Standard). В якості тестів виступили „Тест відомих відповідей” та „Тест Монте Карло”, описані в NIST SP 800-17 та NIST SP 800-20.

За допомогою наступних тестів було згенеровано 3 030 002 байт тестових векторів в режимі ECB (684 122 байт для „Тесту відомих відповідей” та 2 345 880 байт для „Тесту Монте Карло” для зашифрування та розшифрування). Вхідні дані були повністю ідентичні. Генерація векторів для кожного з АРМів тривала протягом близько восьми годин на окремій електронній обчислювальній машині (ЕОМ) на процесорі Intel Celeron D 2.80 GHz. Отриманий на виході весь об'єм даних 2,88 Мб (3 030 002 байт) був ідентичний для усіх трьох АРМів.

Виходячи з цього можна було зробити висновки, що ймовірність відповідності програмних реалізацій АРМів специфікації дуже велика. „Тест відомих відповідей” не є працеміським і виконується за одиниці хвилин на вище описаній ЕОМ. Проте дозволяє провести верифікацію на належному рівні, що доводить використання цього тесту при розробці алгоритму БСШ DES та алгоритмів кандидатів на AES. „Тест Монте Карло” на відміну від „Тест відомих відповідей” є дуже працеміським. Виконується протягом годин. Цей тест є більш надійним. Він дозволяє виконати не тільки верифікацію АРМів на більш високому рівні, але й виявити помилки використання пам'яті при розробці програмного модуля, помилки реалізації багатопоточності та збої операційної системи, на якій тестується даний програмний продукт. Тести є універсальними та дозволяють тестувати будь-які алгоритми БСШ. Програмна модель АРМу тестування на сучасному етапі розроблена тільки для одного алгоритму БСШ, але може легко вдосконалюватись як зовні так і зсередини. У процес вдосконалення може входити як зручний віконний інтерфейс, так і інтеперабельність самого процесу тестування, що дозволить тестувати БСШ різних класів та родин.