Порівняльний аналіз сучасних потокових шифрів

УДК 621.326

Аліна Андрушкевич[1], Марія Дронь[2]

Харківський національний університет радіоелектроніки[1]
Харківський національний університет ім.В.Н. Каразіна[2]
alvasamoilova@gmail.com[1],maria.dron0@gmail.com[2]

На сьогодні поточний шифр європейського стандарту повинен відповідати досить високим показникам – сотні Мбіт/с та навіть декілька Гбіт/с. Ефективне рішення, крім високої продуктивності, повинно володіти такими рисами, як обґрунтованість, доказана надійність шифру, простота та масштабованість, завершеність та ясність алгоритму, а також забезпечувати конфіденційність у каналах передачі інформації.

Метою роботи є порівняльний аналіз сучасних потокових шифрів, визначення відповідності сучасних потокових шифрів сучасним вимогам телекомунікаційних каналів передачі інформації.

У дослідженні були розглянуті всесвітньовідомі криптоалгоритми, які стандартизовані на міжнародному або національному рівні та мають найбільшу довіру.

Зазвичай поточні шифри порівнюються за показниками у швидкості шифрування довгих повідомлень та часу ініціалізації/генерації ключових параметрів. У цій роботі було використано досвід міжнародного конкурсу eSTREAM та всі дослідження потокових шифрів проводились за наступними критеріями:

– Критерій зашифрування довгих потоків, поточні шифри мають найбільш потенційну перевагу над блочними шифрами при зашифруванні довгих потоків. Тому цей показник є важливим критерієм оцінки. У досліджені вимірювався час зашифрування 1Гб даних.

– Критерій зашифрування коротких потоків, цей показник відображає швидкість зашифрування пакетів різної довжини. Кожен виклик функції включає до себе окрему установку вектору ініціалізації (IV), довжина пакетів (40, 576, и 1500 байт) були обрана так, щоб були репрезентивними для телекомунікаційного трафіку. У досліджені вимірювався час зашифрування пакету, швидкість зашифрування байт на мікросекунду та швидкість зашифрування пакетів на мікросекунду.

– Критерій ініціалізації/генерація ключових параметрів. Окремо відображає ефективність встановлення ключа та вектору ініціалізації. Ці два параметра найменш критичні для відображення швидкості зашифрування пакетів так як зневажливо малі порівнюючи з процесом створення та відновлення ключа. При дослідження поточних шифрів були взяті наступні дані: для ключа – 7000 ключових установок (10 ключів на 700 установок на ключ), для вектору ініціалізації – 500 ключових установок (10 ключів на 50 установок); для цих параметрів було зафіксовано загальний час виконання

операцій, скільки затрачено циклів на установку та скільки можливо зробити установок за секунду.

Дослідження за наведеною вище методикою дадуть відповідь, насамперед, на такі важливі питання, як: який потоковий шифр є найшвидшим; який шифр володіє найшвидшою схемою розгортання ключа та який шифр більш адаптований до реалій телекомунікаційного каналу передачі інформації.

Результати попередніх досліджень дали змогу виявити також залежність швидкості шифрування потокових шифрів від збільшення розміру довжини ключа та поставити дуже цікаве запитання перед розробниками.

Якщо «Струмок» є подібний за своєю структурою до «SNOW 2.0», а «SNOW 2.0» є залежність, що при збільшені розміру секретного ключа до 256 біт залишаються високі показники швидкості, навіть більші ніж при 128-бітному розмірі ключа, то можна припустити, що й у «Струмок» повинна зберігатися така тенденція, але ця закономірність не простежується.

Можна зробити припущення, що поточний шифр «Струмок» не набрав своїх справжніх можливостей, є певні апаратні обмеження, які не дають йому певної мірі розкритися.

Попередні результати порівняльного аналізу сучасних потокових шифрів за критерієм шифрування довгих повідомлень представлені на рисунку 1.

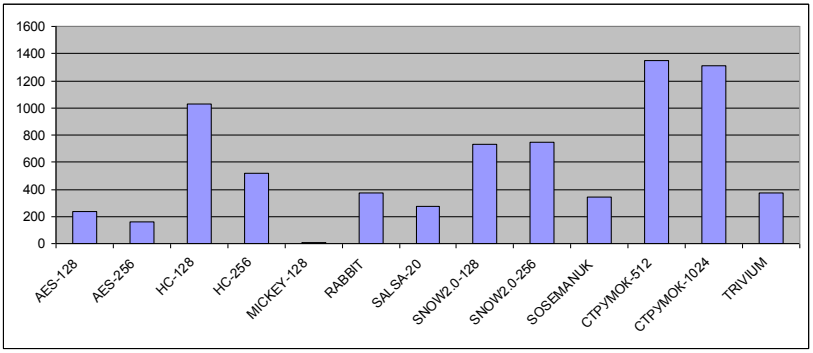

Рис. 1 – Експериментальні результати за критерієм шифрування довгих повідомлень

Науковий керівний – к.т.н. доцент Іваненко Д.В.