ПРИШВИДШЕННЯ ЛІНІЙНИХ ПЕРЕТВОРЕНЬ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ "КАЛИНА"

Мельникова О.А., Стефаниць Е.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні симетричні шифри мають забезпечувати високу швидкість обробки великих обсягів інформації в режимі реального часу. Тому важливим завданням є зменшення обчислювальної складності як базових перетворень шифру (прямого та зворотного) в цілому, так і окремих елементарних перетворень.

Метою доповіді є аналіз можливостей зменшення обчислювальної складності прямого та зворотного лінійних перетворень (перемішувань) змісту стовпців матриці внутрішнього стану для вітчизняного блокового симетричного шифру “Калина” [1, 2].

У доповіді розглянуто як варіанти швидкого виконання базової для вищезгаданих лінійних перетворень операції множення за модулем елементів поля $GF(2^m)$, побудованого за модулем $f(t) = t^8 + t^4 + t^3 + t^2 + 1$, так і різні варіанти реалізації лінійних перетворень в цілому. Зокрема, пропонується використання індексованих таблиць підстановок замість операції множення за модулем елементів поля $GF(2^8)$ та аналізується обчислювальна складність таких варіантів реалізації лінійних перетворень.

Для досягнення максимальної швидкості виконання прямого лінійного перетворення необхідне попереднє обчислення та зберігання таблиці підстановок із 1536 елементів поля, а також використання додаткового індексного масиву із 64 елементів. А для зворотного лінійного перетворення необхідно сформувати таблицю підстановок із 2048 елементів поля та використовувати додатковий індексний масив із 64 елементів.

В доповіді аналізується обчислювальна складність розглянутих варіантів реалізації прямого та зворотного лінійних перетворень і наводяться результати експериментальних вимірювань обчислювальної складності (часу виконання, в тактах процесора). Проведені дослідження показали, що використання запропонованого варіанту індексованих таблиць підстановок дозволяє значно зменшити обчислювальну складність прямого та зворотного лінійних перетворень.

Список літератури

1. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. — Введ. 01-07-2015. — К. : Мінекономрозвитку України, 2015.

2. Горбенко І. Д. Симетричний блоковий шифр "Калина” — новий національний стандарт України / І. Д. Горбенко, Р. В. Олійников, О. В. Казимиров, В. І. Руженцев, О. О. Кузнєцов, Ю. І. Горбенко, О. В. Дирда, В. І. Долгов, А. І. Пушкарьов, Р. І. Мордвінов // Радіотехніка. - 2015. - Вип. 181. - С. 5-22. - Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2015_181_3.