УДК 004.056.055

А. В. Остапенко-Боженова

БАЗОВІ ОЗНАКИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ БЛОКОВИХ ШИФРІВ

Вінницький національний технічний університет

Анотація

Запропоновано визначення набору базових ознак симетричних блокових шифрів, які дозволили класифікувати криптографічні перетворення блокових шифрів.

Ключові слова: шифрування, криптологія, блоковий шифр.

Abstract

The method for determining the set of basic features symmetric block ciphers, which allowed to classify cryptographic transformed block ciphers.

Keywords: encryption, cryptology, block cipher.

Вступ

На сьогоднішній день для покращення основних характеристик симетричних блокових шифрів (СБШ) проводяться дослідження процедури розгортання ключа, режимів блокового шифрування та операцій, що використовуються у функціях раундового перетворення [1].

Одним із сучасних напрямів розробки СБШ підвищеної швидкості є створення псевдонедетермінованих шифрів де формування алгоритмів шифрування відбувається під керуванням секретного параметра [2].

Результати дослідження

Для впровадження ефекту недетермінованості в процес конструювання СБШ доцільно розглянути основні складові елементи блокового шифру.

Для будь якого СБШ можна визначити його базові ознаки:

1. Ознака структури блоку:
   - кількіть підблоків;
   - розрядність підблоків;
2. Ознака функції раунда перетворення (ФРП).

Структура блоку в свою чергу характеризується ознакою його розрядності та ознакою кількості підблоків на які розбивається блок на раундах шифрування.

ФРП характеризується послідовністю застосувань деяких операцій із набору базових операцій СБШ.

Значення ознак можуть бути постійними (C) та змінними (V).

В свою чергу постійні значення означають незмінність ознаки на протязі усіх раундів шифрування та можуть бути:

- залежні від секретного параметра (C_k): конкретне значення ознаки певним чином визначається з обраного секретного параметра (ключа);
- незалежні від секретного параметра (C): конкретне значення ознаки не залежить від значення секретного параметра (ключа).

Змінні значення ознак означають зміну ознаки на всіх (або деяких) раундах шифрування та можуть бути:

- залежними від секретного параметра (V);
- умовно змінним (V_c), коли значення ознаки змінюється відповідно до заданої умови, що не є секретом.

Таблиця 1 - Значення базових ознак СБШ

Ознака структури блоку	Розрядність блоку	Постійна (C)	C	постійне значення розрядності блоку визначене заздалегідь (усі блоки по 128 біт)
			C_k	постійне значення розрядності блоку конкретне значення якого визначається з ключа (усі блоки в залежності від ключа можуть бути: 128, 96, 64 біт)
		Змінна (V)	V	змінне значення розрядності блоку конкретні значення визначаються з ключа (Значення розрядності блоків є змінними залежно від ключа : 1 блок 128 2-й 256 3-й 64)
			V_c	умовно змінне значення розрядності блоку значення яких задаються умовою (задано правило (умова) перші 10 блоків по 64 біт , решта по 128)
	К-ть підблоків на раундах	Постійна (C)	C	постійне значення кількості підблоків на раундах визначене заздалегідь (на всіх раундах по 2 підблоки (мережа Фейстеля) або 4-ри (розширена мережа Фейстеля))
			C_k	постійне значення кількості підблоків на всіх раундах конкретне значення якого визначається з ключа (Залежно від ключа кількість підблоків на всіх раундах може бути 2, 4)
		Змінна (V)	V	змінне значення кількості підблоків на раундах конкретні значення визначаються з ключа (залежно від значення ключа на різних раундах можлива кількість підблоків (2,3,4) пр.. на першому 2 на другому 4 на третьому 2 і т.д.).
			V_c	умовно змінне значення кількості підблоків на раундах значення яких задаються умовою (наприклад для парних раундів 2 підблока для непарних3)
Ознака функції раундового перетворення	ФРП	Постійна (C)	C	постійне значення виду ФРП на всіх раундах визначене заздалегідь (на всіх раундах по додавання за мод2 таблична заміна та таблична перестановка)
			C_k	постійне значення виду ФРП всіх раундах конкретне значення якого визначається з ключа (Залежно від ключа визначається вид ФРП для всіх раундів шифрування)
		Змінна (V)	V	змінне значення виду ФРП на всіх раундах конкретні значення визначаються з ключа (залежно від значення ключа на різних раундах можливі різні види ФРП)
			V_c	умовно змінне значення виду ФРП на раундах, що задаються умовою що не є секретом (наприклад для парних раундів один вид ФРП а для непарних інший)

Виходячи із вищерозглянутої таблиці можна сказати, що описані класи СБШ з точки зору недетермінованості ознак складових криптографічного перетворення відкривають нові можливості до розробки БШ.

Виходячи із розглянутих базових ознак запропонована класифікація СБШ (див.табл.1), що враховує можливість побудови шифрів із змінними значеннями базових ознак.

Висновки

Розглядаючи представників сучасних СБШ [2] можна казати, що більша їх частина відноситься до класу (С, С, С). Тобто усі значення ознак є постійними та заданими для всіх ітерацій. СБШ з керованими операціями відносяться до класу (С, С, V) так як структура ФРП є змінною та залежною від ключових параметрів. СБШ з гетерогенною структурою можна віднести до класу (С, С, C_k).

Запропонований набір базових операцій я дозволяє описати нові класи СБШ, що використовують псевдонедетерміновану послідовність криптопримітивів для подальшого їх дослідження.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Молдовян Н.А. Скоростные блочные шифры / Н.А. Молдовян. — СПб, СПбГУ, 1998. – 212 с.
2. Лужецький В. А. Блочний шифр на основі псевдонедетермінованої послідовності криптопримітивів / В.А. Лужецький, А.В. Остапенко // Науковий вісник ВНТУ. – 2010. – №4. Режим доступу до ел. ресурсу: http://www.nbuv.gov.ua/e-journals/VNTU/2010_4/2010-4.htm
3. Лужецький В. А. Аналіз алгоритмів симетричного блокового шифрування / В.А. Лужецький, А.В. Остапенко // Інформаційні технології та комп'ютерна інженерія. – 2012. – № 3. – С. 55-64.
4. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.

Остапенко-Боженова Аліна Василівна — асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email : ostapenko-bozhenova_a_v@gmail.com

Alina Ostapenko-Bozhenova — Department of Chair Information Protection, Vinnytsia National Technical University, Vinnytsia, email : ostapenko-bozhenova_a_v@gmail.com