найбільш перспективний. Крім того, обґрунтовано доцільність використання взаємного вейвлет-перетворення для математичного методу обробки сигналів для даного методу. Запропоновано алгоритм діагностування роботи двигунів автомобілів на основі оцінки взаємних характеристик їх компонентів та розроблено його функціональну схему.

М. Дьоміна
Науковий керівник – д.т.н., проф. В. С. Глухов

ПЕРЕВІРКА РЕАЛІЗАЦІЇ БЛОКОВОГО СИМЕТРИЧНОГО ШИФРУ «КАЛИНА» ЗА ДОПОМОГОЮ ТЕСТОВИХ ПРИКЛАДІВ

Користувачам глобальних і локальних мереж потрібні засоби захисту інформації, що здатні зберегти конфіденційність, цілісність і доступність. Криптографічний захист цілком відповідає цим вимогам. Одним з способів захисту є блоковий шифр "Калина".

Калина (ДСТУ 7624:2014) – це сучасний новий український стандарт, який підтримує розмір блоку і довжину ключа шифрування 128, 256 і 512 біт, забезпечуючи нормальний, високий та надвисокий рівень стійкості (єдиний у світі стандарт блокового шифрування, що підтримує 512-бітові симетричні ключі). Основні параметри шифру, такі як довжина ключа k і блоку даних l, кількість раундів t та кількість стовпців матриці стану c представлені в табл. 1

Таблиця 1

Довжина блоку (l)	Довжина ключа (k)	Кількість раундів (t)	К-сть стовпців матриці стану (c)
128	128	10	2
256	256	14	4
512	512	18	8

Отже, **актуальною є задача** забезпечення надійного захисту даних за допомогою криптографічного захисту, а саме за допомогою блокового шифру «Калина».

У роботі розглянуто методику перевірки правильності програмної реалізації блокового симетричного криптографічного перетворення:

1) перевірка правильності реалізації усіх базових процедур, визначених у блоковому симетричному шифрі (БСШ) «Калина» (функції розгортання циклових ключів та базових перетворень зашифрування і розшифрування) за допомогою тестових прикладів;

2) перевірка правильності реалізації режимів роботи, визначених визначених у БСШ «Калина» (гамування (CTR); гамування зі зворотнім зв'язком за шифр текстом (CFB); вироблення імітовставки (CMAC); зчеплення шифрблоків (CBC); гамування зі зворотнім зв'язком за шифр гамою (OFB); вибіркове гамування із прискореним виробленням імітовставки (GCM, GMAC); вироблення імітовставки і гамування (CCM); індексованої заміни (XTS); захисту ключових даних (KW)) за допомогою тестових прикладів.

Програмну реалізацію було взято з з git hub за цим посиланням https://github.com/Roman-Oliynykov/Kalyna-reference.

Запропоновано методику тестування:

спочатку перевірялися основні процедури, а потім режими застосування алгоритму симетричного блокового шифру «Калина». Реалізація вважається дійсною, якщо основні процедури та всі реалізовані режими роботи алгоритму були перевірені.

Перевірку реалізації базових перетворень та режимів роботи алгоритму здійснено для різних довжин ключів: 128, 256 або 512 бітів, також для різних довжин блоків: 128, 256 або 512 бітів.

В ході дослідження було використано тестові вектори (які було взято з статті «Новий український стандарт шифрування: Блочний шифр КАЛИНА») для розгортання ключа у циклові ключі, для функцій шифрування, разшифрування та імітовставки (де це використовується) для всіх режимів роботи: проста заміна; гамування; гамування зі зворотнім зв'язком за шифр текстом; вироблення імітовставки; зчеплення шифрблоків; гамування зі зворотнім зв'язком за шифр гамою; вибіркове гамування із прискореним виробленням імітовставки; вироблення імітовставки і гамування; індексованої заміни; захисту ключових даних за допомогою тестових прикладів. При створенні тестових векторів були враховані всі розміри блоку та ключа шифрування, можливість шифрування неповних блоків, до яких використовується функція доповнення блоку, різні розміри параметрів, таких як розмір імітовставки та режим гамування у CFB.

Висновок. У ході роботи було перевірено С-реалізації алгоритму шифрування «Калина», усі наведені тестові приклади було виконано правильно. Це дає змогу перейти до наступного етапу роботи – до імплементації С-описів у ПЛІС засобами Vivado (Xilinx).