НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ННК "Інститут прикладного системного аналізу"
(повна назва інституту/факультету)

Кафедра Системного проектування
(повна назва кафедри)

«На правах рукопису»
УДК 004.056.55:621.391

«До захисту допущено»
Завідувач кафедри
_____ Петренко А.І.
(підпис) (ініціали, прізвище)
___"_____ 2017р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 8.050102 Інформаційні технології проектування
(код і назва спеціальності)

на тему: Дослідження методів протидії аналізу криптосистем при апаратній реалізації RSA

Виконала: студентка 6 курсу, групи ДА-51м
(шифр групи)

Казаченко Ольга Дмитрівна _____ _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник к.т.н., доцент, Капшук О. О._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант з нормконтролю к.т.н., доцент, Кисельов Г. Д. _____
(посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2017 року

Національний технічний університет України
«Київський політехнічний інститут»

Факультет (інститут) ННК «Інститут прикладного системного аналізу» _
(повна назва)

Кафедра Системного проектування
(повна назва)

Рівень вищої освіти – другий (магістерський)

Спеціальність 8.050102 Інформаційні технології проектування
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Петренко А.І.
(підпис) (ініціали, прізвище)
«___»_____2017 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Казаченко Ольги Дмитрівни

1. Тема дисертації Дослідження методів протидії аналізу криптосистем при апаратній реалізації RSA

Науковий керівник дисертації Капшук О. О. к.т.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджено наказом по університету від «_20_»___03____ 2017 р. №32-ст

2. Термін подання студентом дисертації 12.06.2017

3. Об'єкт дослідження Сторонні канали, та інформація яку вони несуть під час роботи криптосистеми

4. Предмет дослідження Методи протидії аналізу інформації, отриманої по стороннім каналам

5. Перелік завдань, які потрібно розробити

- Провести огляд аналізу сигналів, що будуть отримані
- Провести огляд криптосистеми RSA
- Дослідити існуючі атаки, що базуються на інформації, отриманої по стороннім каналам
- Проаналізувати основні, існуючі методи протидії аналізу сторонніх каналів

- Розробити пристрій, що допомагає збирати інформацію для аналізу
- Запропонувати результативний метод протидій аналізу криптосистем по стороннім каналам

6. Орієнтовний перелік ілюстративного матеріалу презентація на тему «Дослідження методів протидії аналізу криптосистем при апаратній реалізації RSA »

7. Орієнтовний перелік публікацій :

- Казаченко О. Д. Side-channel analysis of cryptosystems, Мультидисциплінарний науковий журнал «Інтернаука», Випуск 7, 2017
- Казаченко О. Д. Реалізація алгоритму RSA з застосуванням китайської теореми про залишки, Мультидисциплінарний науковий журнал «Інтернаука», Випуск 7, 2017

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	Доц., к.т.н. Капшук О. О.		

9. Дата видачі завдання 30.09.2016

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Отримання завдання	30.09.2016	
2	Збір інформації	25.01.2017	
3	Дослідження та аналіз вимог завдання, вибір доступних рішень для вирішення поставленої задачі	01.03.2017	
4	Огляд архітектурної бази для реалізації алгоритму	12.03.2017	
5	Розробка схеми та створення приладу для дослідження	28.03.2017	
6	Аналіз замінюваних результатів	12.04.2017	
7	Дослідження ефективності існуючих методів протидії та виведення результатів	28.04.2017	
8	Робота над розділом розроблення стартап-проекту	21.05.2017	
9	Оформлення дипломної роботи	02.06.2017	
10	Отримання допуску до захисту та подача роботи в ДЕК	12.06.2017	

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

на магістерську дисертацію

виконану на тему: Дослідження методів протидії аналізу криптосистем при апаратній реалізації RSA.

студентом: Казаченко Ольгою Дмитрівною

Робота виконана на 118 сторінках, містить 47 ілюстрацій, 24 таблиці. При підготовці використовувалася література з 41 різних джерел.

Актуальність

Комп'ютери та інші електронні пристрої на сьогодні тісно пов'язані з людським життям. Насправді вони супроводжують нас усюди і несуть велику кількість інформації про свого власника. Такий великий попит техніки та використання її як в робочих потребах так і у власних вплинуло на розвиток механізмів захисту приватної інформації користувачів, збереженню її конфіденційності.

Головні механізми у захисті інформації у наш час спрямовані на забезпечення двох основних моментів: цілісності та конфіденційності. Починаючи з середини минулого століття цими ідеями опікувалась наука – криптографія. Її розвиток вилився у створення багатьох алгоритмів шифрування, які з рокам удосконалювались розвитком технологій та математичного апарату і на сьогодні досягли можливості виконати вимоги до збереження даних.

У даній роботі зосереджено увагу на RSA алгоритмі, що використовується для збереження конфіденційності інформації, цифрових підписів та у протоколі TLS при передачі даних через інтернет. Широкого поширення алгоритм здобув й в апаратній реалізації на вбудованих пристроях, таких як мобільні телефони і навіть у смарт-картах.

Мета

Метою даної дипломної роботи є дослідження існуючих методів протидії аналізу криптосистем, за інформацією, що несуть сторонні канали, а також

дослідження цієї інформації за допомогою розробленого приладу, на тестовій апаратній реалізації RSA.

Завдання

Для досягнення мети були поставлені наступні завдання:

- Провести огляд аналізу сигналів, що будуть отримані;
- Провести огляд криптосистеми RSA;
- Дослідити існуючі атаки, що базуються на інформації, отриманої по стороннім каналам;
- Проаналізувати основні, існуючі методи протидії аналізу сторонніх каналів;
- Розробити пристрій, що допомагає збирати інформацію для аналізу;
- Запропонувати результативний метод протидій аналізу криптосистем по стороннім каналам;

Об’єкт дослідження

Об’єктом дослідження було обрано сторонні канали та інформація, яку вони несуть при роботі криптосистеми.

Предмет дослідження

Предметом дослідження в даній роботі є методи протидії аналізу інформації по стороннім канали, їх вплив на реалізацію алгоритму, його швидкодію та надійність, яку вони гарантують.

Методи досліджень

Проведення аналізу інформації зібраної по стороннім каналам, а також методів протидії аналізу цієї інформації та перевірка їх ефективності при використанні в апаратній реалізації криптосистеми RSA.

Наукова новизна

Наукова новизна роботи полягає в:

1. Виробленні рекомендацій щодо вибору методів протидії аналізу криптосистеми по стороннім каналам, для гарантування надійності роботи криптосистеми RSA.
2. Виробленні рекомендацій щодо застосуванню методів протидії в залежності від поставлених вимог до роботи алгоритму, та вибраної платформи для реалізації криптосистеми.

Практична цінність

Практична цінність роботи проявляється в тому, що був розроблений засіб для дослідження інформації по стороннім каналам криптографічних систем та новий метод протидії. За допомогою нього можна перевірити всі існуючі методи протидії аналізу криптосистем.

Результат даної роботи можна використовувати в подальшому для створення нових методів протидії аналізу криптосистем по стороннім каналам.

Ключові слова

Сторонні канали, спектральний аналіз, криптосистема, Side-channel analysis , RSA, SPA, DPA, cryptosystem.

РЕФЕРАТ

на магистерскую диссертацию

выполненную на тему : Исследование методов противодействия анализу криптосистем при апаратной реализации RSA .

студентом: Казаченко Ольгой Дмитривной

Работа выполнена на 118 страницах, содержит 47 иллюстрации, 24 таблицы. При подготовке использовалась литература из 41 разных источников.

Актуальность

Компьютеры и другие электронные устройства на сегодня тесно связаны с человеческой жизнью. На самом деле они сопровождают нас повсюду и несут большое количество информации о своем владельце. Такой большой спрос техники и использования ее как в рабочих нуждах так и в собственных повлияло на развитие механизмов защиты частной информации пользователей, сохранению ее конфиденциальности.

Главные механизмы в защите информации, в наше время, направлены на обеспечение двух основных моментов: целостности и конфиденциальности. Начиная с середины прошлого века этими идеями занималась наука - криптография. Ее развитие вылился в создание многих алгоритмов шифрования, с годам совершенствовались развитием технологий и математического аппарата и на сегодня достигли возможности выполнить требования к сохранению данных.

В данной работе сосредоточено внимание на RSA алгоритме, который используется для сохранения конфиденциальности информации, цифровых подписей и в протоколе TLS при передаче данных через интернет. Широкое распространение метод получил и в аппаратной реализации на встроенных устройствах, таких как мобильные телефоны и даже в смарт-картах.

Цель

Целью данной работы является исследование существующих методов противодействия анализу криптосистем, по информации, которую несут

сторонние каналы, а также исследования этой информации с помощью разработанного прибора, на тестовой аппаратной реализации RSA.

Задание

Для достижения цели были поставлены следующие задачи:

- Провести обзор анализа сигналов, которые будут получены;
- Провести обзор криптосистемы RSA;
- Исследовать существующие атаки, основанные на информации, полученной по сторонним каналам;
- Проанализировать основные, существующие методы противодействия анализу сторонних каналов;
- Разработать устройство,которое помогает собирать информацию для анализа;
- Предложить результативный метод противодействия анализу криптосистем по сторонним каналам;

Объект исследования

Объектом исследования было выбрано сторонние каналы и информация, которую они несут при работе криптосистемы.

Предмет исследования

Предметом исследования в данной работе являются методы противодействия анализу информации по сторонним каналам, их влияние на реализацию алгоритма, его быстродействие и надежность, которую они гарантируют.

Методы исследований

Проведение анализа информации собранной по сторонним каналам, а также методов противодействия анализу этой информации и проверка их эффективности при использовании в аппаратной реализации криптосистемы RSA.

Научная новизна

Научная новизна работы заключается в:

1. Разработке рекомендаций по выбору методов противодействия анализу криптосистемы по сторонним каналам, для обеспечения надежности работы криптосистемы RSA.

2. Разработка рекомендаций по применению методов противодействия в зависимости от поставленных требований к работе алгоритма, и выбранной платформы для реализации криптосистемы.

Практическая ценность

Практическая ценность работы заключается в том, что был разработан способ для исследования информации по сторонним каналам криптографических систем и новый метод противодействия. С помощью него можно проверить все существующие методы противодействия анализа криптосистем.

Результат данной работы можно использовать в дальнейшем для создания новых методов противодействия анализа криптосистем по сторонним каналам.

Ключевые слова

Сторонние каналы, спектральный анализ, криптосистема, Side-channel analysis , RSA, SPA, DPA, cryptosystem.

ABSTRACT

on master's thesis

on topic: Investigation of methods for countering the analysis of cryptosystems in the hardware implementation of RSA.

Student: Kazachenko Olha

Work carried out on 118 pages containing 47 figures, 24 tables. The paper was written with references to 41 different sources.

Relevance

Computers and other electronic devices today are closely related to human life. In fact, they accompany us everywhere and carry a lot of information about their owner. Such a large demand for equipment and its use both in working needs and in its own way has influenced the development of mechanisms for protecting the privacy of users, preserving its confidentiality.

The main mechanisms in the protection of information, in our time, are aimed at providing two main capabilities: integrity and confidentiality. Since the middle of the last century, these ideas have been engaged in science - cryptography. Its development resulted in the creation of many encryption algorithms, improved with the development of technologies and mathematical apparatus over the years, and today have achieved the ability to meet the requirements for data protection.

In this paper, attention is focused on the RSA algorithm, which is used to preserve the confidentiality of information, digital signatures and in the TLS protocol when transmitting data over the Internet. The method was widely used in hardware implementation on embedded devices, such as mobile phones and even smart cards.

Goal

The purpose of this thesis is to study the existing methods of countering the analysis of cryptosystems, according to the side-channel information, and also to study this information with the help of the developed instrument, on a test hardware implementation of RSA.

Task

To achieve the goal, the following tasks were set:

- Review the analysis of signals to be received;
- Conduct a review of the RSA cryptosystem;
- Investigate existing attacks based on side-channel information;
- Analyze the main existing methods of countering the side-channel analysis;
- Develop a device that helps to gather information for analysis;
- Offer an effective method for countering the side-channel analysis of cryptosystems;

Object of study

The object of the study was selected side-channels and information that they carry during the work of the cryptosystem.

Subject of study

The subject of the research in this paper are methods of counteracting the analysis of side-channel information, their impact on the implementation of the algorithm, its speed and reliability, which they guarantee.

Research methods

Analyzing the side-channel information, as well as methods of counteracting the analysis of this information and checking their effectiveness when used in the hardware implementation of the RSA cryptosystem.

Scientific novelty

The scientific novelty of the work:

1. Development of recommendations on the choice of methods for countering the side-channel analysis of the cryptosystem, to ensure the reliability of the RSA cryptosystem.

2. Development of recommendations on the use of countermeasures, depending on the requirements for the operation of the algorithm, and the chosen platform for implementing the cryptosystem.

Practical value

The practical value of the work is manifested in the fact that has been developed a device for side-channel analysis of cryptographic systems and a new method of counteraction. With the help of it, you can check all existing methods of countering the analysis of cryptosystems.

The result of this work can be used in the future to create new methods for countering the side-channel analysis of cryptosystems.

Keywords

Spectral analysis, Side-channel analysis , RSA, SPA, DPA, cryptosystem.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AES	- Advanced Encryption Standard ;
RSA	- Rivest, Shamir та Adleman;
TLS	- Transport Layer Security;
ЦОС	- Цифрова Обробка Сигналів;
СЧАН	- Спектрально-Частотний Аналіз;
STFT	- Short-Time Fourier Transform;
CRT	- Chinese Remainder Theorem;
SCA	- Side Channel Analysis;
SPA	- Simple Power Analysis;
DPA	- Differential Power Analysis;
EMA	- Electro Magnetic Analysis;
SoC	- System on Chip;
SHA	- Secure Hash Algorithm;
BIOS	- Build-In Operation System;
RTOS	- Real-Time Operation System;
ADC	- Analog – Digital Convert

ВСТУП

Комп’ютери та інші електронні пристрої на сьогодні тісно пов’язані з людським життям. Насправді вони супроводжують нас усюди і несуть велику кількість інформації про свого власника. Такий великий попит техніки та використання її як в робочих потребах так і у власних вплинуло на розвиток механізмів захисту приватної інформації користувачів, збереженню її конфіденційності.

Головні механізми у захисті інформації у наш час спрямовані на забезпечення двох основних моментів: цілісності та конфіденційності. Починаючи з середини минулого століття цими ідеями опікувалась наука – криптографія. Її розвиток вилився у створення багатьох алгоритмів шифрування, які з рокам удосконалювались розвитком технологій та математичного апарату і на сьогодні досягли можливості виконати вимоги до збереження даних.

Головними стандартами шифрування даних у наш час являються:

- Симетричне AES (128, 256) шифрування;
- Асиметричне RSA шифрування.

При вірній реалізації алгоритму забезпечується надійне шифрування інформації за досить помірний час його виконання. Ці алгоритми зараз являються частиною багатьох протоколів обміну даними та використовуються для шифрування інтернет-трафіку.

У даній роботі зосереджено увагу на RSA алгоритмі, що використовується для збереження конфіденційності інформації, цифрових підписів та у протоколі TLS при передачі даних через інтернет. Широкого поширення алгоритм здобув й в апаратній реалізації на вбудованих пристроях, таких як мобільні телефони і навіть у смарт-картах.

Розвиток криптографії завжди стимулювався намаганнями зловмисників подолати та пробити діру у реалізованій системі захисту. І так як сам алгоритм

являється відкритим, це створило ряд можливих підходів до розкриття зашифрованих даних, починаючи з повного перебору ключів до атак з вибірковим вхідним текстом. Таким чином алгоритми завжди мали балансувати на межі часу за який вони шифрують данні та часу який зловмисники мають витратити на їх дешифровку відомими атаками. Це спонукало розвивати математичний апарат алгоритмів і перераховані вище забезпечують високу швидкість при часі дешифровки, за умов що ключ шифрування невідомий, більш ніж 10и років. Саме тому вони являються сьогоденним стандартом і використовуються всюди. Тому знайти у них вади та зламати їх криптостійкість – справжній виклик для фахівців у цій сфері.

Безперечно тема роботи є актуальною для багатьох вбудованих систем, адже всі вони підтримують апаратну реалізацію RSA. Також вся інформація, що шифрується алгоритмом, є конфіденційною і дуже важливу гарантувати її безпеку.

Об’єктом дослідження є криптосистема RSA та методи її захисту від аналізу по живленню. Предметом дослідження є шляхи поліпшення стійкості алгоритму при його апаратній реалізації.

Так як математичний апарат алгоритму RSA дуже складний набагато легше атакувати його через середу у якій він працює. Таким чином метою даної роботи є дослідження існуючих методів захисту та апаратних рішень для криптосистеми RSA, що гарантують її стійкість перед можливими атаками через середу у якій вона реалізована. Ця мета досягається шляхом аналізу різних рішень апаратної реалізації алгоритму на мікроконтролері та спостереженні за поведінкою середовища та зміні її показників безпосередньо при шифруванні даних.

На сьогодні вже існують роботи по даній темі, більшість з них були написані одним з винахідників алгоритму в процесі вдосконаленнях існуючих реалізацій. Вони ще не являються широко розповсюдженими і зараз таку дослідження мають велику популярність в різних інститутах по всьому світу. У роботі будуть розглянуті деякі з вже існуючих рішень та запропонований

новий. Нажаль багато з вже існуючих не вирішують проблему в цілому, вони лише ускладнюють аналіз криптосистеми. Нижче розглянуто практично отримані результати роботи існуючих рішень та проаналізовано, які з них можуть покращити реалізацію криптосистеми RSA.

1 ОСНОВИ ЦИФРОВОЇ ОБРОБКИ СИГНАЛІВ

Вступ

При аналізі криптосистеми використовують дані заміряні по стороннім каналам. Вони являють собою сигнал, що характеризує виконувану операцію по одному з критеріїв: по часу, по споживання чи по електромагнітному випромінюванню.

Аналіз отриманих даних споріднений з аналіз простого сигналу в цифровій обробці сигналів. В даному розділі розглядаються підходи, що використовуються в аналізі криптосистем.

Так як заміряний сигнал являє собою неперіодичний сигнал, то потребує додаткових дій для результативної обробки. Насправді, отриманий нами сигнал містить частотні гармоніки, що характеризують природу виконуваних операцій. Найкраще аналіз частот, що в ньому присутні виконується шляхом розкладання сигналу в частотний спектр. Зазвичай для цього використовують перетворення Фур‘є. Враховуючи, що сигнал неперіодичний, для перетворення використовують віконну функцію, щоб збільшити точність отриманих частот.

Особливості віконних функцій та частотний спектр сигналу, отриманий перетворенням Фур’є – частина цифрової обробки сигналів, що потрібна у виконуваному дослідженні.

1.1 Основні поняття ЦОС

Сигнал – це фізичний процес, що несе інформацію у своїх параметрах. Він описується як деяка функція від часу *f(t)* або від просторових координат *f(x, y).* Сигнал, що буде розглядатись у роботі – одновимірний сигнал функцій часу. Сигнали бувають:

- Неперервні або дискретні по рівню чи часу;
- Детерміновані чи випадкові;
- Періодичні або неперіодичні;

- Скінченної тривалості або безкінечні;

Цифрова обробка сигналів дозволяє представляти сигнали у вигляді послідовності дискретних значення, квантова них по амплітуді. Таким чином сигнал легше зберігати та представляти результати обробки зберігаючи при цьому високу завадо захищеність цифрового сигналу [1].

Серед основних напрямів цифрової обробки даних, що будуть використовуватися у дослідженні варто розглянути наступні:

1. Статична обробка сигналу: аналіз статичних параметрів та його кореляції для оцінки стану джерела сигналу (наприклад демодуляція – перетворення сигналу в символи);
2. Непараметрична обробка сигналу: покращення його характеристик фільтрацією, апроксимацією, інтерполяцією, тощо (наприклад для зменшення рівня шуму, відновлення втрачених фрагментів);
3. Аналіз сигналів в частотно-часовій чи частотній області з використанням дискретних перетворень для аналізу структурних особливостей складних систем (наприклад для виявлення закономірносте в часових рядах)[3];

Для виконання поставлених задач перед системам ЦОС буде використана система обробки сигналів без вимог до роботи в реальному часі, реалізована на базі персонального комп’ютера з відповідним програмним забезпеченням, а саме програмою Audacity.

Основною характеристикою, що може бути обчислена для сигналів з скінченою енергією на інтервалі часу *T,* є енергія сигналу

$$E(t) = \int_{t-T/2}^{t+T/2} x^2(t)dt \quad .$$

Для переходу від формул для неперервних сигналів до дискретних здійснюється заміна інтегралу на суму, а довжини часового інтервалу – на кількість відліків:

$$E(t_i) = \sum_{k=0}^{N} x^2(t_i)$$.

1.2 Спектральне представлення сигналу

Будь-який неперервний періодичний сигнал *x(t)* з періодом *T* може бути представлений у вигляді ряду Фур'є

$$x(t) = \frac{1}{2}\sum_{k=-\infty}^{\infty} C_k e^{jk\omega t} = \frac{C_0}{2} + \sum_{k=1}^{\infty} |C_k| \cos(k\omega t + \varphi_k),$$

де $\omega = \frac{2\pi}{T} = 2\pi f$ - основна циклічна частота, а комплексні коефіцієнти обчислюються прямим перетворенням Фур'є:

$$C_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} x(t)\cdot e^{-jk\omega t}dt =$$

$$\frac{2}{T}\left[\int_{-\frac{T}{2}}^{\frac{T}{2}} x(t)\cdot\cos(k\omega t)dt - j\int_{-\frac{T}{2}}^{\frac{T}{2}} x(t)\cdot\sin(k\omega t)dt\right] =$$

$$= a_k - jb_k,\ k = 0,\pm1,\pm2,\pm3...$$

Дійсна та уявна частини комплексних коефіцієнтів можуть бути обчислені як

$$a_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{N}{2}} x(t)\cdot\cos(k\omega t)dt,$$

$$b_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{N}{2}} x(t)\cdot\sin(k\omega t)dt.$$

Коефіцієнт b_0 завжди дорівнює нулю, а коефіцієнт a_0 дорівнює постійній складовій сигналу:

$$a_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{N}{2}} x(t)dt\,.$$

Комплексні коефіцієнти також представляються у вигляді

$$C_k = |C_k| \cdot e^{j\varphi_k},$$

де

$|C_k| = \sqrt{a_k{}^2 + b_k{}^2}$ - амплітуда *k*-ї гармонічної складової, а її фаза:

$$\varphi_k = \arg(C_k) = -arctg\left(\frac{b_k}{a_k}\right).$$

Таким чином, періодичний неперервний сигнал представляється у вигляді суми гармонічних складових з частотами, кратними основній частоті сигналу. Сукупність амплітуд комплексних коефіцієнтів ряду Фур'є називається амплітудним спектром, а сукупність їх фаз – фазовим спектром.

Перетворення Фур'є має наступні важливі особливості:

- Лінійність: спектр суми сигналів дорівнює сумі спектрів, а при зміні амплітуди сигналу спектр змінюється у стільки ж разів, не змінюючи форму;
- При зсуві сигналу по осі часу змінюється лише фазовий спектр (амплітудний залишається незмінним);
- Спектр періодичного сигналу дискретний, а дискретного – періодичний;

Якщо сигнал не є періодичним, він представляється інтегралом Фур'є:

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} S(j\omega)\cdot e^{j\omega t}d\omega,$$

де $S(j\omega) = \int_{-\infty}^{\infty} x(t)\cdot e^{-j\omega t}dt$ - комплексний спектр,

$A(\omega) = |S(j\omega)|$ - амплітудний спектр,

$\varphi(\omega) = \arg(S(j\omega))$ - фазовий спектр.

Таким чино, для неперіодичного сигналу функція спектру є неперервною. Однак при цифровій обробці і сигнал і його спектр представляються скінченною послідовністю дискретних відліків. Це означає, що сигнал фактично приймають за періодичний із періодом, рівним тривалості вибірки, що обробляється [2].

Величина $|S(j\omega)|^2$ називається спектральною щільністю потужності. Зв'язок між потужностями сигналу, представленого в часовій та частотній області, визначає теорема Парсеваля:

$$\int_{-\infty}^{\infty} x^2(t)dt = \int_{-\infty}^{\infty} |S(j\omega)|^2 d\omega .$$

При цифровій обробці сигналу використовується теорема Фур'є, за формулами із відповідних неперервних аналогів при заміні інтегралу сумою:

$$a_k = \frac{1}{N}\sum_{i=0}^{N-1} x_i \cdot \cos(2\pi \frac{i}{N}k),$$

$$b_k = \frac{1}{N}\sum_{i=0}^{N-1} x_i \cdot \sin(2\pi \frac{i}{N}k),$$

$i=0,1,...,N;\ k=0,1,...,N/2.$

Тут N – кількість відліків, $x_i = x(t_i)$ – дискретний відлік неперервного сигналу $x(t)$ в момент часу $t_i = i*\Delta t$, де Δt – інтервал дискретизації ($f_d = 1/\Delta t$ – частота дискретизації)[3].

Зворотнє перетворення Фур'є записується наступним чином:

$$x_i = \frac{1}{2}\sum_{k=0}^{N-1} C_k e^{jk\cdot 2\pi \frac{i}{N}} = \frac{C_0}{2} + \sum_{k=1}^{N/2-1} |C_k| \cos(k2\pi \frac{i}{N} + \varphi_k)$$

Інколи як для прямого, так і для зворотнього перетворення застосовують нормуючий коефіцієнт перед знаком суми $\frac{1}{\sqrt{N}}$, щоб задовільнити нерівність Парсеваля [4].

Коефіцієнту з номером k відповідає значення частоти $f_k = k \cdot \frac{f_d}{N}$. Таким чином, коефіцієнти дискретного перетворення Фур'є обчислюються для діапазону частот від 0 до частоти дискретизації сигналу.

Маючи *N* відліків сигналу, можна отримати лише *N* незалежних коефіцієнтів, що описують сигнал в частотній області. Оскільки коефіцієнти, отримані в результаті дискретного перетворення Фур'є є комплексини, то незалежними будуть лише *N/2* цих коефіцієнтів, що відповідає частотам від 0 до половини частоти дискретизації. Враховуючи, що спектр періодичний для дискретного сигналу і симетричний відносно осі ординат, коефіцієнти від *N/2* до *N-1* є «дзеркальним відображенням» перших *N/2* коефіцієнтів відносно половини частоти дискретизації, що й зображено на Рисунку 1.1. Для аналізу сигналу в частотній області беруть лише першу половину такого спектру.

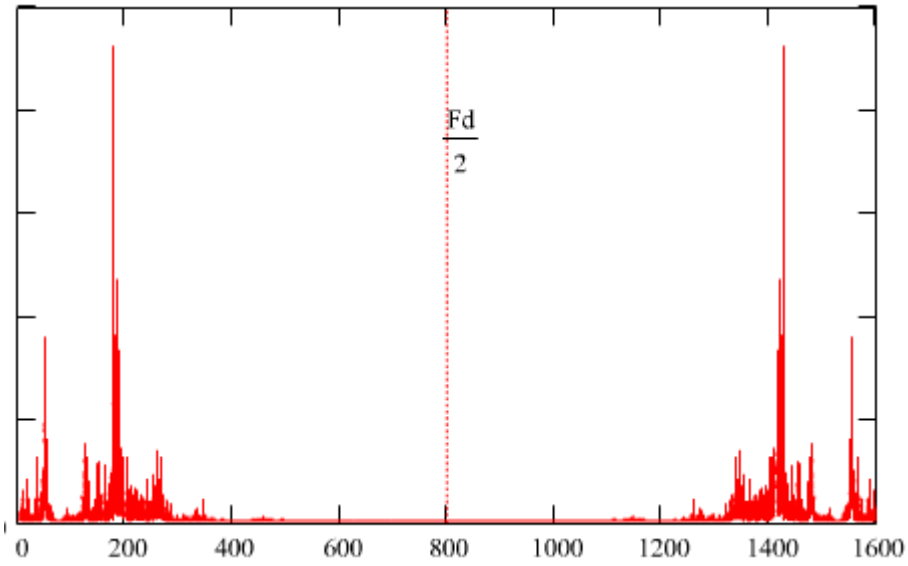


Рисунок 1.1 – Амплітудний спектр оцифрованого сигналу

1.3 Поняття дискретизації сигналу

Дискретизація сигналу – це заміна неперервного в часі сигналу *x(t)* на послідовність його дискретних відліків *x(k · Δt),* взятих у моменти часу, кратні інтервалу дискретизації *Δt*. Величина *Fd = 1/Δt* називається частотою дискретизації сигналу [5].

Вибір частоти дискретизації здійснюється з врахуванням спектрально-кореляційних властивостей сигналу. Мінімально допустима частота дискретизації, при якій сигнал теоретично можливо відновити без втрат, визначається теоремою Котельникова: $F_d \geq 2F_m$..

Точне відновлення сигналу при цьому забезпечується пропусканням послідовності дискретизованих відліків через ідеальний фільтр низької частоти.

Якщо частота дискретизації вибрана меншою, ніж за теоремою Котельникова виникне явище накладання спектрів дискретизованого сигнал, або аліасинг [8]. На Рисунку 1.2 показано приклад неперервного сигналу, що містить дві частотні складові – 1кГц та 40 кГц та результат дискретизації з частотою 44100 кГц (позначені квадратиками та пунктирною лінією). Можемо побачити, що в дискретизованому сигналі зникла складова з частотою 40 кГц, однак з'явилась паразитна гармоніка за рахунок оцифрування цієї складової через інтервали, дещо більші за її період.

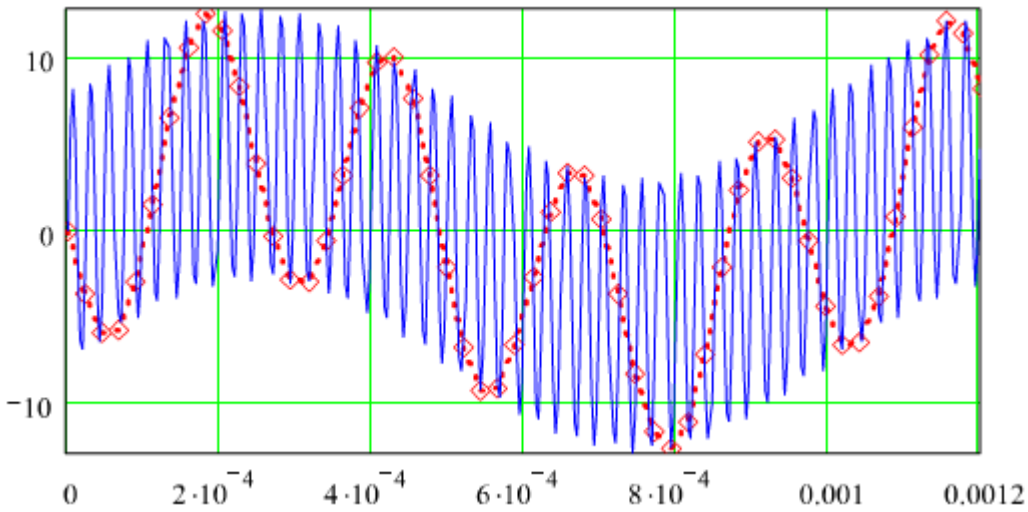


Рисунок 1.2 – Ефект аліасингу

На Рисунку 1.3 зображено спектр сигналу, дискретизованого за теоремою Котельникова й видно максимуми на частотах 1кГц та 40 кГц. На Рисунку 1.4 – умови теореми Котельникова не виконані – складова 40 кГц присутня, однак властивості періодичності спектру дискретного сигналу та симетричності

амплітудного спектру відобразили її відносно частоти 22,05 кГц (половина частоти дискретизації) на частоту близько до 5 кГц. Також ця паразитна гармоніка проглядається на Рисунку 1.1.

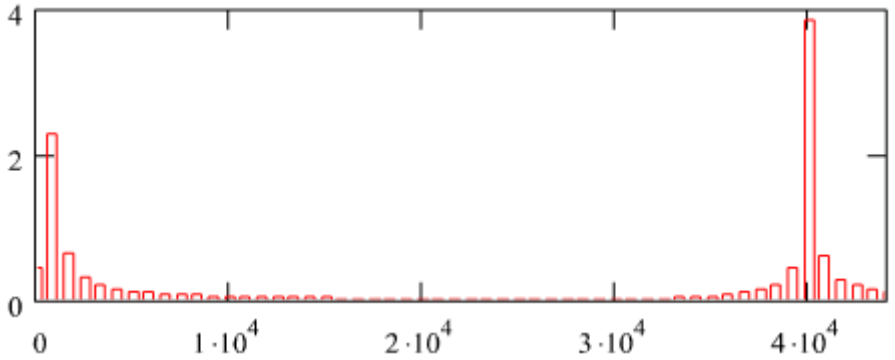


Рисунок 1.3 – Виконання теореми Котельникова (F_d=384 кГц)

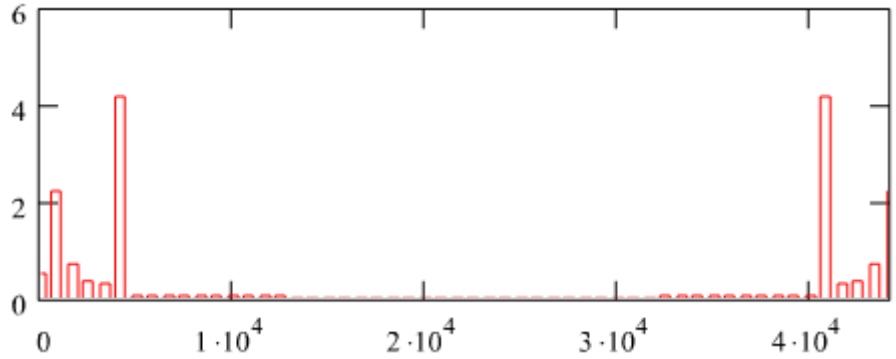


Рисунок 1.4 – Порушення теореми Котельникова (F_d=44,1 кГц)

Для гарантованого усунення аліасингу слід пропустити ще аналоговий сигнал через фільтр низьких частот із частотою зрізу, рівною половині частоти дискретизації. Таким чином усунуться всі складові, які могли б перетворитись на паразитні гармоніки. Звичайно застосування такого фільтру приводить до

втрати частини інформації, що міститься у високочастотних складових сигналу, однак гарантує його коректну дискретизацію із необхідною частотою.

1.4 Віконне перетворення Фур'є

Перетворення Фур'є, як і інші ортогональні перетворення, мають зміст для сигналів, що є стаціонарними. Для сигналів, статичні характеристики яких змінюються в часі, перетворення Фур'є буде відображати лише усереднене структуру сигналу [6]. Так, якщо в деякий момент часу у сигналі виникло короткочасне високочастотне коливання, то в результуючому спектрі, обчисленому для достатньо довгої вибірки, на даній частоті буде пік відносно невеликої амплітуди, що має всі шанси загубитися на фоні шумів. Інший приклад наведено на Рисунку 1.5, де чітко видно, що для першого фрагменту сигналу частотні складові на частотах 1500-2500 Гц практично відсутні, в той час як по спектру, обчисленому по всій вибірці, здогадатись про це неможливо (Рисунок 1.6).

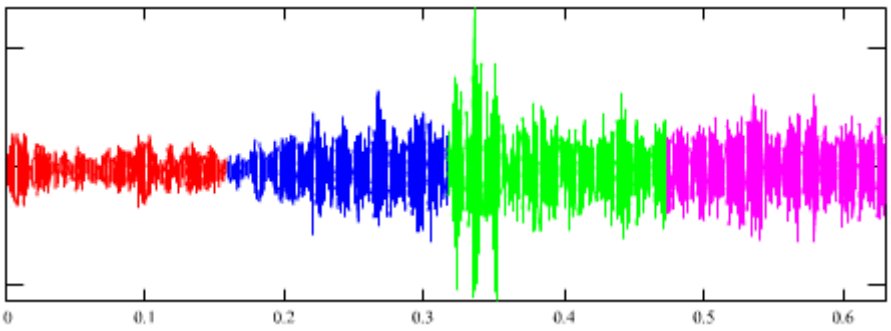


Рисунок 1.5 – Сигнал

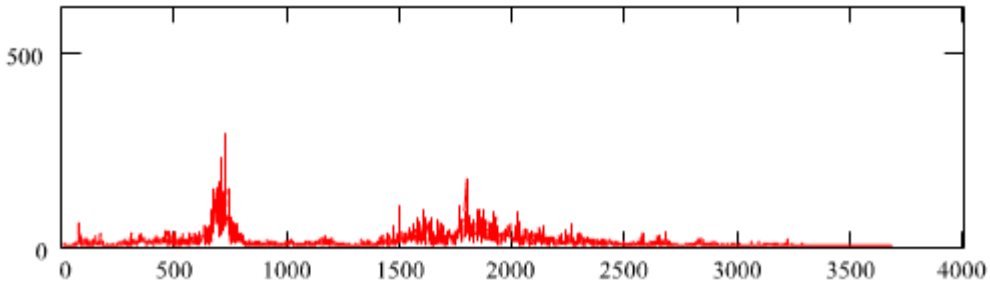


Рисунок 1.6 – Спектр, обчислений по всій довжині реалізації

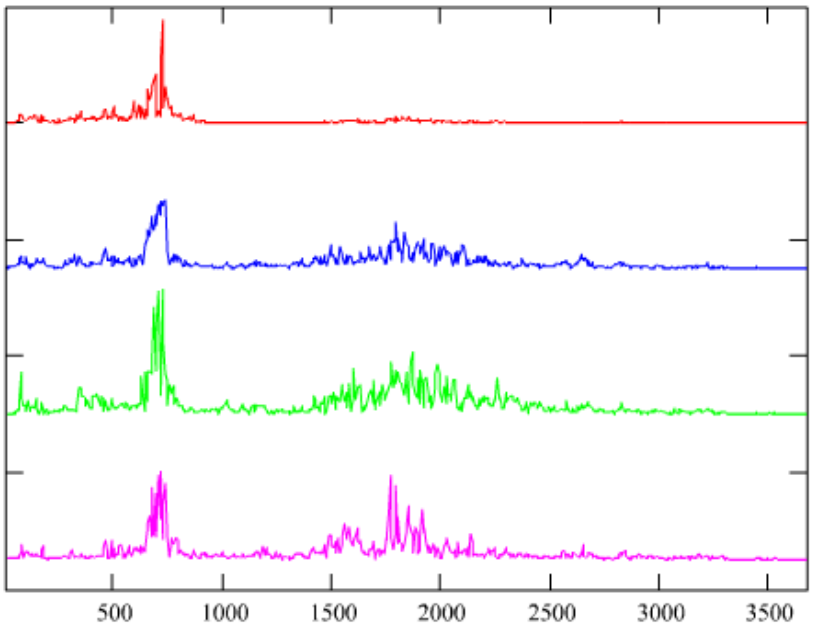


Рисунок 1.7 – Спектри, обчислені по послідовним фрагментам

Це можна вирішити шляхом розділення вибірки на фрагменти невеликого розміру, та обчисленням для кожного з них перетворення Фур'є окремо, як показано на Рисунку 1.7 для сигналу з Рисунку 1.5. Таким чином, результатом такої обробки сигналу буде являтися двовимірний масив, координатами якого будуть час (з інтервалом дискретизації рівним тривалості одного фрагмента) та частота. Таке представлення має назву – представлення у частотно-часовій області (Рисунок 1.8).

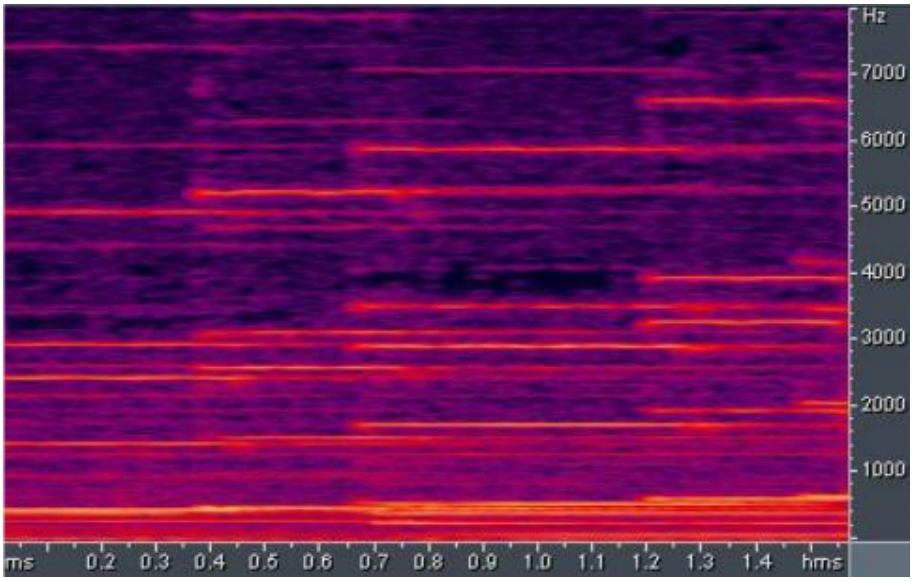


Рисунок 1.8 – Представлення у частотно-часовій області

Якщо при поінтервальному обчисленні спектру застосувати формули перетворення Фур'є без будь-яких вдосконалень, це означатиме періодичне продовження кожного із фрагментів сигналу на всю часову вісь. Тим часом у первинному сигналі продовженням деякого фрагменту сигналу є не його копія, а сусідні фрагменти сигналу. Таким чином, обчислений спектр буде відрізнятись від «істинного» спектру даного фрагменту, так як в місцях з'єднання копій фрагменту з'являться розриви. Їх наявність спричинятиме появу нових паразитних частотних складових, яких точно не було в первинному сигналі. В результаті енергія кожної спектральної складової буде частково змазаною по всьому спектру. Це явище має назву – «розтікання спектру» [1]. Уникнути цього можна лише при умові, що значення сигналу та його похідних на початку і в кінці інтервалу співпадають, як зображено на Рисунку1.9.

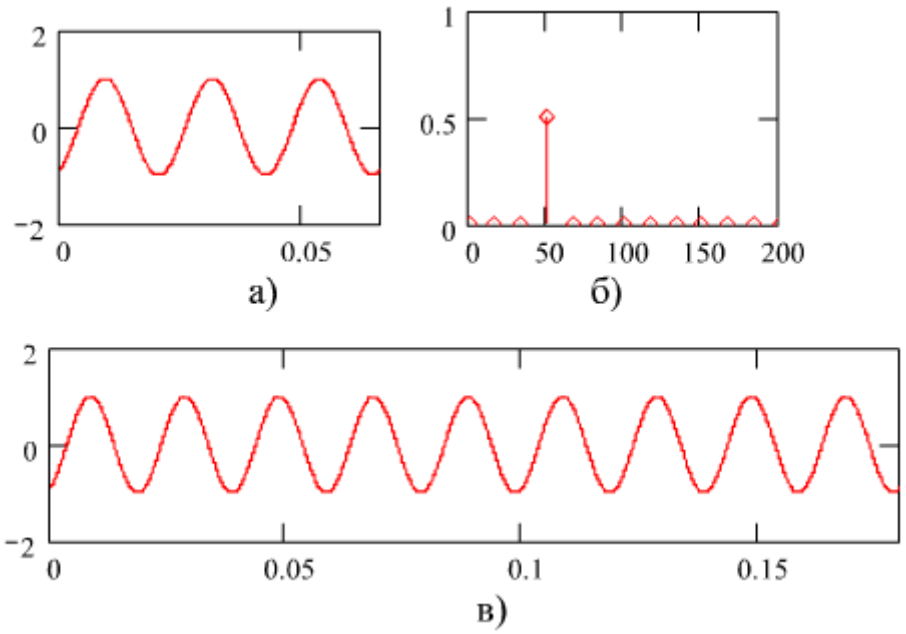


Рисунок 1.9 – Фрагмент сигналу (а) та його спектр (б), для первинного сигналу (в)

Якщо ж для аналізу взяти інтервал інакше, то це спричинить виникнення розривів у періодично продовженому сигналі та згадане вище явище розтікання спектру (Рисунок 1.10).

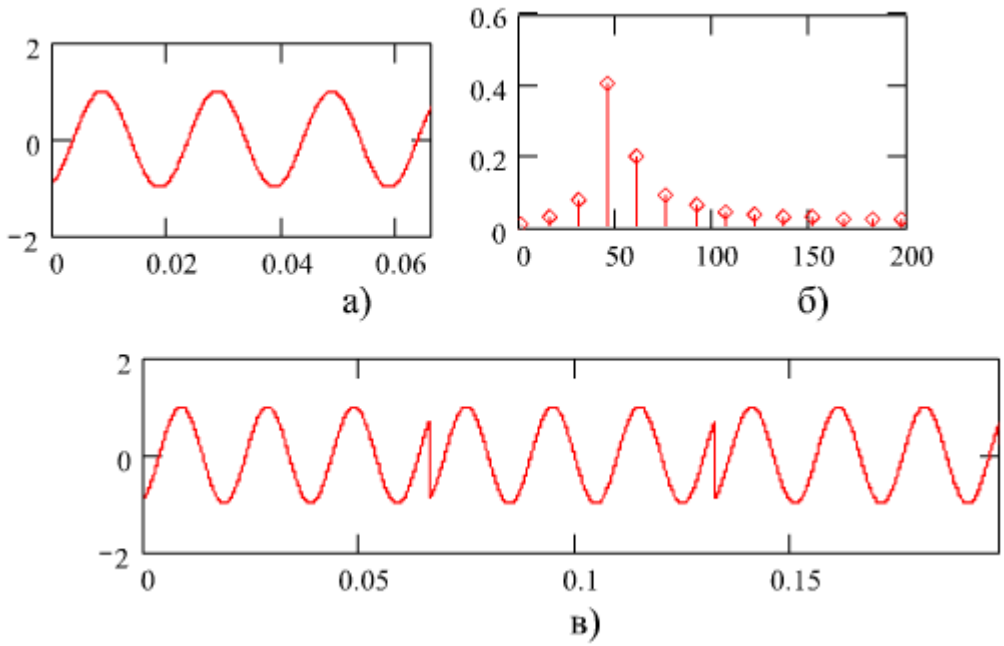


Рисунок 1.10 – Фрагмент сигналу (а) та його спектр (б), для первинного сигналу (в)

Щоб згладити це явище, застосовують так звану функцію вікна на яку можна помножити фрагмент сигналу перед здійсненням перетворення Фур'є. Функція вікна приймає максимальне значення в середині досліджуваного фрагменту сигналу, прямує до нуля на його границях і дорівнює нулю за його межами. За рахунок цього на початку і в кінці інтервалу зважений сигнал плавно спадає до нуля, і його періодичне продовження не призведе до появи розриву сигналу в місці сполучення фрагментів[7].

Перетворення Фур'є, застосоване до послідовних фрагментів сигналу, зважених функцією вікна

$$STFT(\omega,\tau) = \int_{-\infty}^{\infty} x(t)\cdot w(t-\tau)\cdot e^{-j\omega t}dt,$$

де *w(t)* – функція вікна, τ – момент часу, для якого обчислюється перетворення, називають короткочасним перетворенням Фур'є (скорочено STFT). Інтервал для якого обчислюється короткочасне перетворення Фур'є, також інколи називають вікном.

Дискретне STFT

$$STFT_{i,k} = \sum_{n=0}^{N-1} x_{j+n}\cdot w_n \cdot e^{-jk\frac{n}{N}2\pi}.$$

Найчастіше при обчисленні STFT застосовуються наступні функції вікна:

1. Хемінга

$$w_n = 0.54 - 0.46\cos\frac{2\pi\cdot n}{N-1};$$

2. Ханна

$$w_n = 0.5\left(1-\cos\left(\frac{2\pi\cdot n}{N-1}\right)\right);$$

3. Блекмана

$$w_n = 0.42 - 0.5\cos\frac{2\pi\cdot n}{N-1} + 0.08\cos\frac{4\pi\cdot n}{N-1};$$

4. Бартленна

$$w_n = \frac{2}{N-1} \cdot \left(\frac{N-1}{2} - \left| n - \frac{N-1}{2} \right| \right);$$

5. Крайзера

$$w_n = \frac{I_0(\alpha\sqrt{1-(\frac{2n}{N-1})^2})}{I_0(\alpha)},$$

де $I_0(t)$ – функція Бесселя першого роду нульового порядку :

$$I_0(t) = 1 + \sum_{n=1}^{\infty} \left[\frac{1}{n!} (\frac{t}{2})^n \right]^2.$$

Звичайне дискретне перетворення Фур'є (без функції вікна) можна розглядати як застосування прямокутного вікна, тобто $w_n = 1$.

Розглянемо як застосування функції вікна впливає на результат обчислюваного спектру сигналу. Як зазначалось раніше, важливою властивістю перетворення Фур'є є те, що згортка сигналів в часовій області відповідає добутку їх перетворень Фур'є, а добуток сигналів в часовій області відповідно – згортці перетворень Фур'є. Таким чином множення сигналу на функцію вікна призводить до згортки спектру сигналу із спектром віконної функції. В результаті, якщо спектр сигналу в дійсності складається із послідовності дискретних компонент на частотах w_k

$$S^*(\omega) = \sum_{k=0}^{N} A_k \delta(\omega - \omega_k),$$

то обчислений дискретний спектр, завдяки властивості згортки із дельта-функції та лінійності операції згортки, буде являти собою

$$S(\omega) = S^*(\omega) \otimes W(\omega) = \sum_{k=0}^{N} A_k \cdot (\delta(\omega - \omega_k) \otimes W(\omega) = \sum_{k=0}^{N} A_k \cdot W(\omega),$$

де $W(w)$ – спектр функції вікна.

Тобто, кожен дискретний компонент, що у істинному спектрі мав форму дискретної дельта-функції, набуває форми спектру функції вікна.

Типові форми спектрів для перерахованих вище функцій вікна зображені на Рисунках 1.11 – 1.16.

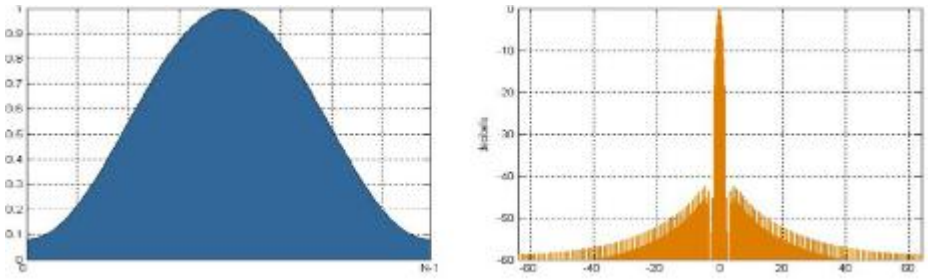


Рисунок 1.11 – Вікно Хеммінга та його спектр

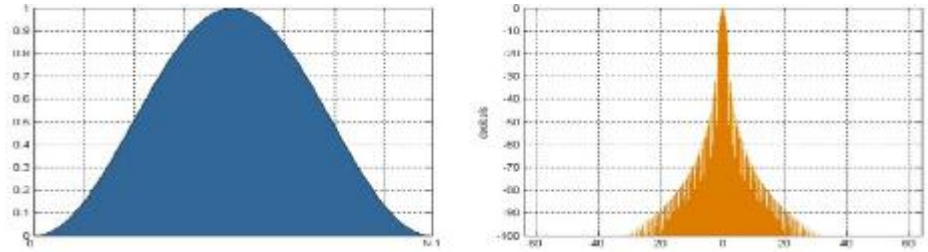


Рисунок 1.12 – Вікно Ханна та його спектр

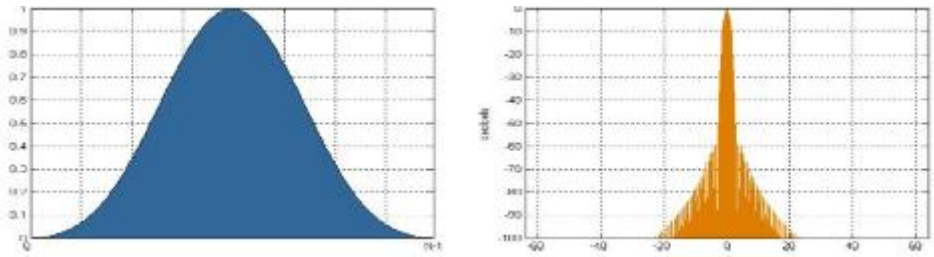


Рисунок 1.13 – Вікно Блекмана та його спектр

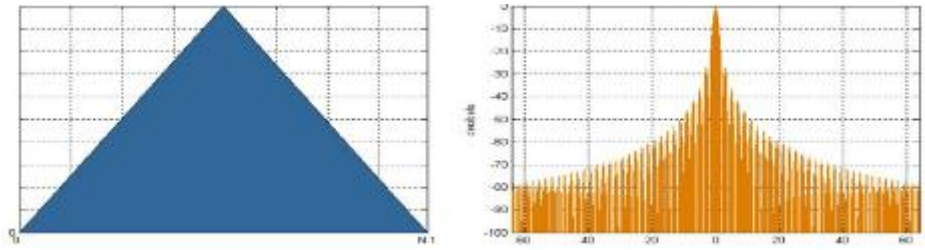


Рисунок 1.14 – Вікно Бартлетта та його спектр

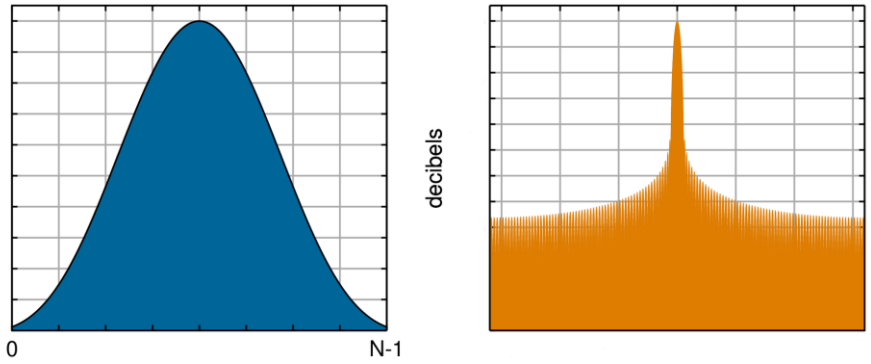


Рисунок 1.15 – Вікно Крейзера та його спектр (α = 2)

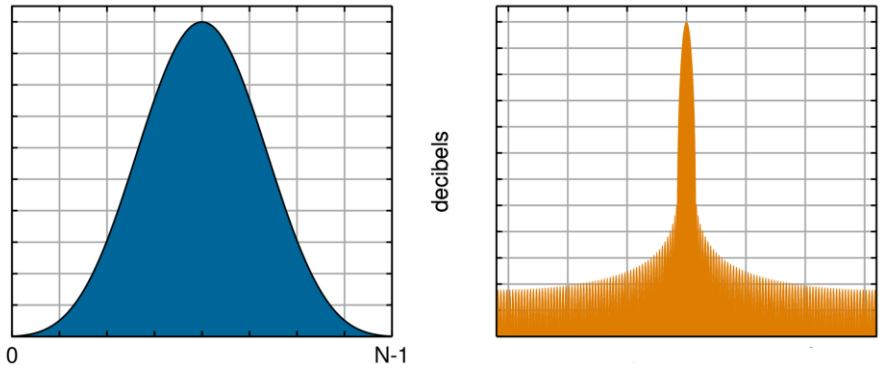


Рисунок 1.16 – Вікно Крейзера та його спектр (α = 3)

Вибір функції вікна для аналізу здійснюється виходячи з того, що є більш пріоритетним: виділення окремих спектральних компонент на фоні шумів без обов'язкової вимоги до точності визначення їх частоти, чи точне виділення близьких по частоті спектральних компонент. В першому випадку важливим є мінімальна амплітуда бокових пелюсток спектру вікна, а в другому – їх максимально швидке затухання. У Таблиці 1.1 наведені характеристики функцій вікна, які, як видно є взаємно виключними. Або функція вікна зменшує загальний рівень шуму, або забезпечує низький рівень бокових пелюсток. Відносним компромісом є вікно Хеммінга (Рисунок 1.11), що забезпечує погіршення відношення сигнал/шум на рівні з вікном Бартлетта (Рисунок 1.14) та Ханна (Рисунок 1.12), й при цьому характеризується меншим рівнем бокових пелюсток [1].

Таблиця 1.1 – Характеристики функцій вікна

Функція вікна	Рівень бокових пелюсток, дБ	Швидкість затухання бокових пелюсток, дБ/октаву	Еквівалентна ширина частотної смуги бокових пелюсток, відліки	Погіршення відношення сигнал/шум порівняно з вхідним сигналом, дБ
Хеммінга	-43	-6	1.36	3.10
Ханна	-32	-18	1.50	3.18
Бартлетта	-27	-12	1.33	3.07
Блекмана ($\alpha = 0.16$)	-58	-18	1.73	3.01
Крайзера ($\alpha = 3.0$)	-69	-6	1.80	3.56
Крайзера ($\alpha = 3.5$)	-82	-6	1.93	3.74
Прямокутне	-13	-6	1.00	3.92

Під еквівалентною шириною частотної смуги бокових пелюсток в Таблиці 1.1 мається на увазі відношення ширини частотної смуги вікна до ширини частотної смуги прямокутного вікна (Рисунок 1.17).

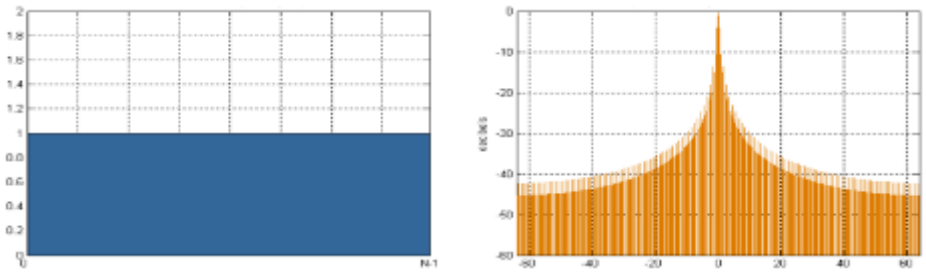


Рисунок 1.17 – Прямокутне вікно та його спектр (вікно відсутнє)

Застосування функції вікна призводить до того, що частина інформації, що містилась в сигналі на краях інтервалу, фактично втрачається. Щоб уникнути втрати цієї інформації, віконне перетворення Фур'є зазвичай обчислюють для інтервалів, що частково перекриваються. При цьому коефіцієнт перетворення зазвичай вибирають в межах 0.5 – 0.75.

Важливим параметром віконного перетворення Фур'є є тривалість, тим більшою є роздільна здатність по часу. Разом з тим, оскільки із N дискретних відліків сигналу неможливо отримати більше ніж N незалежних коефіцієнтів ортогонального перетворення, роздільна здатність по частоті

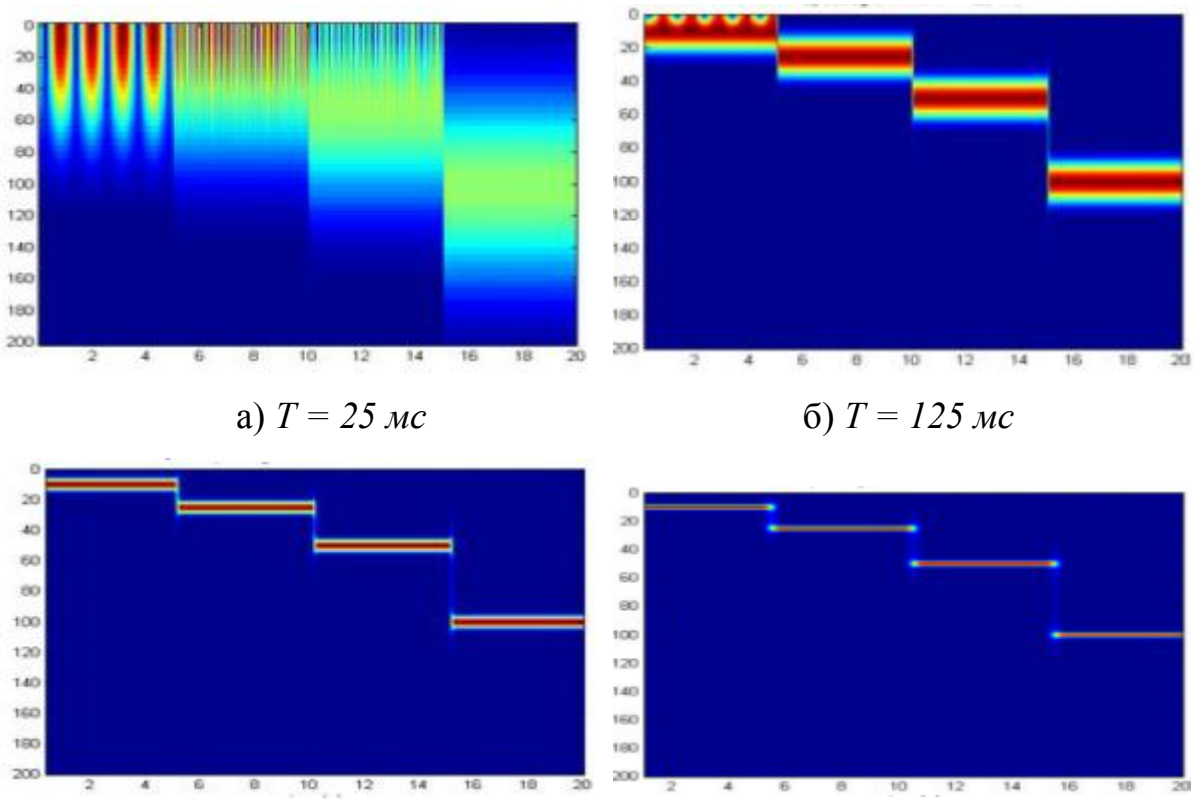
$$\Delta f = \frac{F_d}{N}$$

буде тим гіршою, чим менше відліків сигналу містить інтервал. Таким чином, при використанні STFT неможливо одночасно забезпечити високу роздільну здатність як по часу, так і по частоті. Інколи це пов'язують їз принципом невизначеності Гейзенберга. Таким чином, якщо у сигналі присутня складова деякої частоти, то можна або точно локалізувати її в часі або визначити її частоту.

На Рисунку 1.18 показані STFT для різної довжини вікон для сигналу

$$x(t) = \begin{cases} \cos(2\pi 10t)\,;\ 0 \le t < 5s \\ \cos(2\pi 25t)\,;\ 5 \le t < 10s \\ \cos(2\pi 50t)\,;\ 10 \le t < 15s \\ \cos(2\pi 100t)\,;\ 15 \le t < 20s \end{cases}$$

Для малої ширини вікна (Рисунок 1.18 (а) та (б)) точність визначення частоти є дуже низькою, що видно в розмитих максимумах, при цьому границі переходів між різними частотами чітко виділяються. Для достатньо довгої ширини вікна (Рисунок 1.18 (в) та (г)) частоти локалізуються достатньо точно, але на межах переходів між ними складно з високою точністю визначити момент переходу [9].



а) *T = 25 мс* б) *T = 125 мс*

В) *T = 375 мс* г) *T = 1000 мс*

Рисунок 1.18 – Результат STFT для різних довжин вікна

Таким чином, віконне перетворення Фур'є забезпечує найбільш адекватну оцінку спектра нестаціонарного сигналу, однак потребує детального підбору довжини вікна та функції вікна в залежності від вирішуваної задачі.

1.5 Поняття про спектрально-часовий аналіз

Спектрально-часовий аналіз (СЧАН) – це метод дослідження нестаціонарних випадкових сигналів, що полягає в оцінці „потокового" спектра частини сигналу, що відповідає ковзному часовому вікну деякої малої довжини. При подібній оцінці виходить залежність спектра потужності сигналу, як від частоти, так і від положення (середини або правого краю) вікна. Ця залежність візуалізується у вигляді або двовимірних ліній рівнів, або тривимірних рельєфів, які називають СЧАН–діаграмами. Максимальним значенням такої залежності відповідають періоди часу збільшення потужності коливань у тих або інших частотних смугах. СЧАН часто застосовується для виявлення

нестаціонарних сигналів у дискретних у часі протяжних випадкових процесах [9].

Будується спектрограма в такий спосіб. Часове вікно довжиною в задану кількість відліків ряду зміщується уздовж ряду зліва направо із заданим кроком. Для кожного кроку розраховується спектр потужності фрагмента ряду, що потрапив у вікно. Одержаний спектр потужності розгортається уздовж осі ординат зі значенням абсциси, відповідної до положення середини вікна. У результаті виходить залежність оцінки спектра потужності від двох параметрів у вигляді рельєфу, а саме, від частоти й від положення часового вікна. Слідкуючи за хребтами на рельєфі можна одержати уявлення про те, як інтенсивність прояву тієї або іншої циклічності змінювалася за часом (Рисунок 1.19).

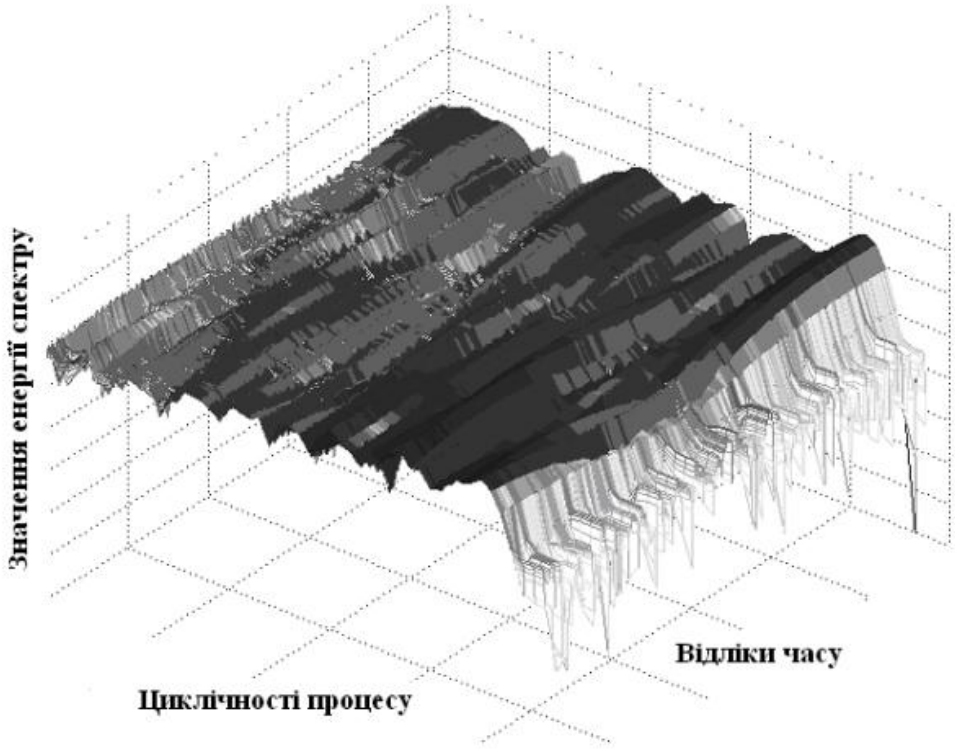


Рисунок 1.19 – Тривимірна СЧАН-діаграма

Зіставляючи звичайне й віконне перетворення Фур’є можна дійти висновку про те, що останнє розв’язало всі проблеми з аналізом і синтезом функцій і сигналів. Але принцип невизначеності Гейзенберга, відомий з курсу

фізики, говорить про те, що неможливо одночасно одержати високе часове і частотне відрізнення, що вже згадувалось раніше. Вибираючи вікно з малою шириною за часом, одержимо високе часове відрізнення і низьке частотне, вибираючи вікно з великою шириною за часом, одержиме високе частотне відрізнення і низьке часове. Віконне перетворення Фур'є оперує з вікнами однакової ширини й тому дане протиріччя для нього нерозв'язне. І, крім того, у ньому використовується єдина базисна функція – синусоїда – з усіма властивими їй недоліками й, виходить, недоліками перетворення Фур'є:

– незастосовність до аналізу нестаціонарних сигналів, у яких певні частотні компоненти існують тільки в певні проміжки часу або коли параметри сигналів змінюються в часі;

– перетворення Фур'є навіть для однієї заданої частоти вимагає знання сигналу не тільки в минулому, але й у майбутньому, що є теоретичною абстракцією;

– в умовах практично неминучого обмеження числа гармонік або спектра коливань точне відновлення сигналу після прямого та зворотного перетворень Фур'є теоретично і практично неможливо через наявність ефекту Гібса;

– базисною функцією при розкладанні в ряд Фур'є є гармонійне коливання, яке математично визначене в нескінченному інтервалі часу та має незмінні в часі параметри;

– при чисельному інтегруванні в нескінченних межах при прямому та зворотному перетворенні відповідно в часовий і в частотній області виникають значні обчислювальні труднощі;

– істотні особливості сигналу у вигляді розривів або піків викликають несуттєві зміни частотного образу сигналу у всьому нескінченному інтервалі частот, які „розмазуються" по всій частотній осі, що робить їхнє виявлення в спектрі практично неможливим;

– навіть умоглядно зрозуміло, що плавна синусоїдальна базисна функція в принципі не може представляти перепади сигналів з нескінченною крутістю, хоча на практиці подібні імпульсні сигнали застосовуються дуже широко;

– єдине пристосування до визначення швидких змін сигналів – це різке збільшення кількості гармонік, які, однак, впливають на форму сигналу й за межами локальних особливостей сигналу;

– по складу вищих гармонік спектра практично неможливо оцінити місце розташування особливостей на часовій залежності сигналу і їх характер;

– для нестаціонарних сигналів при прямому та зворотному перетворенні Фур'є суттєво збільшується обчислювальна складність.

Висновки

В даному розділі було розглянуто обробку неперіодичного сигналу віконним перетворенням Фур'є.

З отриманої інформації треба врахувати, що при аналізі заміряного сигналу, віконне перетворення може надати точні дані для однієї з характеристик : локалізувати частоту у часі, або точно визначити її значення. При замірі сигналу спожитої потужності нам неважливо коли саме у часі сталась та чи інша періодика. Нам важлива з точністю визначити її значення.

Крім того використовувати в аналізі краще усього віконне перетворення Хеммінга, як компромісне. Насправді найважливішим показником для нас являється відношення сигнал/шуму, тому можливо буде використане й вікно Ханна.

Треба брати до уваги, що дуже важливо правильно підібрати ширину вікна. Найвлучнішим варіантом є використовувати приблизно $T = 350\text{-}400$ *мс*. Таким чином не з'являються паразитні частоти, й при цьому досить чітко видно значення частот.

2 АНАЛІЗ КРИПТОСИСТЕМ ТА МЕТОДИ ПРОТИДІЇ

Вступ

Даний розділ охоплює дуже великий обсяг інформації, що стосується аналізу криптосистем по стороннім каналам та криптосистеми як такої. По-перше, розглянута сама криптосистема, ідея яку вона втілює та специфіка ти схеми шифрування.

В основі роботи біло розглянуто саме цей алгоритм, адже він найбільше піддається атакам по стороннім каналам через низьку швидкодію та при цьому являється досить популярним на вбудованих пристроях, які також легше всього аналізувати за сторонніми каналами. Вирішення питання швидкодії часто відбувається шляхом використання китайської теореми про залишки. Вона також буде розглянута нижче, та її вплив на роботи алгоритму.

Після розгляду об’єкту дослідження перейдемо до аналізу його характеристики, які зазвичай використовуються зловмисниками. Є цілий ряд відомих підходів, які експлуатують інформацію отриману по стороннім каналам. Найбільшу увагу заслуговують атаки по споживанню, адже вони можуть привести до розкриття приватного ключа, що являє на сьогодні більшу цінність ніж досягнення відмови роботи системи.

Звичайно увагу буде приділено і атак по часу, що можуть характеризувати виконувані дії. Також розглянуті атаки за помилками, які з більшою ймовірністю призведуть до відмови системи ніж до викриття даних. І в кінець кінців, електромагнітні атаки, що потребують досить точне та складне обладнання для втілення у життя.

В кінці розділу пропонуються деякі види захисту від розглянутих вище атак, які можуть бути реалізовані на мікроконтролерах як апаратно так і програмно, і навіть фізично. Запропоновані також нові методи протидії, що захищають від аналізу по споживанню криптосистеми.

2.1 Алгоритм RSA

У 1978 році Рон Ривест, Аді Шамір і Леонард Адлеман представили криптографічний алгоритм, який міг би замінити менш захищений NBS (National Bureau of Standards). Головне, що RSA реалізує криптосистему з публічним ключем, а також цифрові підписи. Створення RSA стимулювалось, опублікованними за декілька років до цього, роботами Діффі і Хеллмана, які описали ідею такого алгоритму, але не розробляли його [10].

Введений в той час, коли ера електронної пошти, як очікувалось, найближчим часом настане, RSA реалізовував дві важливі ідеї:

1. Шифрування з відкритим ключем. Ця ідея опускає необхідність «кур'єра» доставити ключі одержувачів через інший безпечний канал перед передачею повідомлення. В RSA, ключі шифрування відкриті, а ключі дешифрування ні, таким чином, тільки людина з правильним ключем розшифровки зможе розшифрувати зашифроване повідомлення. Кожна людина має свої власні ключі шифрування і дешифрування. Ключі повинні бути зроблені таким чином, що ключ дешифрування не може бути легко отриманий з відкритого ключа.

2. Цифрові підписи. Отримувачу може знадобитися перевірити, що отримане повідомлення насправді було від очікуваного відправника (підпис), а не тільки що звідти (аутентифікація). Це робиться за допомогою ключа дешифрування відправника і підпис згодом може бути перевірений ким-небудь, використовуючи відповідний ключ шифрування. Таким чином, підписи не можуть бути підроблені. Крім того, жоден з підписувачів не може пізніше заперечувати, що підписав повідомлення. Це не тільки корисно для електронної пошти, але і для інших електронних транзакцій та передач, таких як грошові перекази.

На сьогодні криптосистема RSA використовується у різних продуктах, на різних платформах і у багатьох галузях. В даний час вона вбудовується в комерційні продукти, число яких постійно збільшується. Також її

використовують операційні системи Microsoft, Apple, Sun і Novell. В апаратному виконанні RSA алгоритм застосовується в захищених телефонах, на мережних платах Ethernet, на смарт-картах. Математичний апарат, що лежить в основі роботи алгоритму дуже складний і базується на обчислювальній складності задачі факторизації великих цілих чисел.

Криптографічні системи з відкритим ключем використовують так званні односторонні функції, котрі характеризуються наступними властивостями:

- Якщо відомо *x*, то *f(x)* відносно легко розрахувати
- Якщо відомо $y = f(x)$, то для того щоб розрахувати *x* немає легко та ефективного шляху

Під односторонністю мається на увазі не теоретична одно направленість, а практична неможливість розрахувати оберне значення з використання сучасних обчислювальних засобів за прийнятний час.

В основі криптосистеми покладена задача факторизації добутку двох великих чисел. Для шифрування потрібно реалізувати операцію піднесення у степінь великого числа по модулю, а для дешифрування необхідно обчислити функцію Ейлера від великого числа, для чого потрібно знати розклад числа на прості множники.

2.1.1 Криптосистема з відкритим ключем

Кожен користувач має свої власні процедури шифрування і дешифрування, *E* і *D*. Ці процедури пов'язані з ключами, які, в RSA зокрема, походять з двох спеціальних чисел. Почнемо з повідомлення - *M*, яке й потрібно зашифрувати. Є чотири процедури, які є специфічними і необхідними для криптосистеми з відкритим ключем:

а) Розшифровка зашифрованого повідомлення дає вихідне повідомлення, зокрема, $D\ (\mathrm{E}\ (\mathrm{M})) = \mathrm{M}$.

б) Реверсія процедури все ще повертає *M:* $\mathrm{E}\ (D\ (M)) = \mathrm{M}$.

в) *E* і *D* легко обчислити.

г) Відкритість *E* не ставить під загрозу таємність *D*, це означає, що ви не можете легко отримати, *D* з *E*.

При заданому *E*, все ще не можливо ефективно обчислити *D*. Якщо $C = E(M)$ - шифротекст, то намагання з'ясувати, *D*, намагаючись знайти таке *M*, що $E(M) = C$ - невиправдано складно: число тестових повідомлень було б непрактично великим.

E, яке задовольняє умові (а), (в) і (г) називається «пастка односторонньої функції». Це пастка, тому що, так як зворотне *D* легко обчислити, якщо певна «лазівки» в інформації доступна, але в іншому випадку важко. Це один-шлях, тому що це легко обчислити в одному напрямку, але важко в іншому. Це перестановка, тому що вона задовольняє (б), тобто, кожен шифротекст є потенційним повідомленням, і кожне повідомлення є зашифрованим текстом будь-якого іншого повідомлення. Ствердження (б), насправді необхідне для забезпечення підписів.

Тепер ми переходимо до конкретних ключів, і уявляємо користувачі A і B (Алісі і Боб) на криптосистемі двох відкритих ключів: E_A, E_B, D_A, D_B.

2.1.2 Забезпечення приватності

Шифрування, яке зараз використовується, як спосіб приватної передачі повідомлення, робить це так, що ніякий зловмисник не зможе обійти шифротекст, який, по суті, являється білим шумом. Без власності (г), проте, процес шифрування ще не з відкритим ключем, як стандарт NBS. Це вимагає доставки ключів іншим приватним способом, який представляє собою додатковий процес, який перевершить NBS. Таким чином, RSA є відмінною відповіддю на цю проблему. Таким чином, ефективний метод обчислення *D* повинен бути знайденим, таким чином, щоб зробити RSA повністю автономним і надійним. Для того, щоб він був надійним, він повинен використовувати просту арифметику, яка легко обчислюється (вимога пункту (в)) на комп’ютерах загального призначення.

Тепер Боб хоче відправити приватне повідомлення для Аліси. Він буде отримувати E_A з публічного файлу, шифрувати M, отримуючи $C = E_A(M)$, після чого Аліса розшифровує його своїм власним D_A, який тільки вона може зробити, відповідно до властивості (г). Вона може також відповісти Бобу, використовуючи E_B. Таким чином, все, що потрібно, це угода для користувачів бути частиною криптосистеми шляхом розміщення їх даних шифрування в загальнодоступні файли. Немає необхідності в своєчасному зв'язку, приватному чи ні. Крім того, завдяки властивості (г), жоден перехоплювач не може вивести D від прослуховування E.

2.1.3 Цифровий підпис

Для повної впевненості, що повідомлення сформоване відправником, а не тільки переслане через нього третьою стороною, яка могла використати такий самий ключ шифрування, нам потрібен цифровий підпис разом з прийнятим повідомленням. Це має очевидні наслідки, які мають важливе значення в реальних додатках.

Боб хоче відправити приватне повідомлення для Аліси. Для того, щоб підписати його, ми робимо невеликий трюк, за умови, що алгоритм RSA є швидким і надійним, в основному за рахунок властивості (в). Ми дешифруємо повідомлення з ключем Боба, що допускають властивості (а) і (б), які стверджують, що кожне повідомлення шифротекст ще одного повідомлення, і що кожен шифротекст може бути інтерпретовано як повідомлення. Формально,

$$D_B(\mathrm{M}) = S$$

Потім ми шифруємо S ключем шифрування Аліси.

$$\mathrm{E}_\mathrm{A}(S) = \mathrm{E}_\mathrm{A}(D_B(\mathrm{M}))$$

Таким чином, ми можемо гарантувати, що тільки вона може розшифрувати документ. Коли вона його розшифровує, вона отримує підпис $D_\mathrm{A}(E_\mathrm{A}(D_B(M))) = S$. Тепер вона знає, що повідомлення прийшло від Боба, так як тільки його ключ дешифрування може обчислити підпис. Повідомлення не

повинно бути відправлено окремо, так як Аліса може отримати його з підпису, використовуючи відкрити ключ шифрування Боба, тобто

$$E_B(S) = E_B(D_B(M)) = M.$$

Так як *S* залежить від *M*, а зашифрована передача Боба залежить від *S*, ми отримуємо відправку даних, що залежать як від повідомлення так і від підпису й можуть бути виведені з переданого документу.

Це гарантує, що повідомлення не може бути, так як модифіковане M у вигляді M' породило б підпис $S' = D_B(\mathrm{M}')$, що неможливо, так як D_B не відоме з властивості (г) [10].

Так що Аліса не тільки володіє доказом того, що Боб підписав повідомлення і справді відправив його, але вона також не може змінити *M*, підробивши підпис для будь-якого іншого повідомлення.

2.1.4 Математична база

До сих пір очікується, що *E* і *D* легко обчислити за допомогою простої арифметики. Повідомлення повинно бути представлено чисельно цілим від *0* до *n - 1*. Якщо повідомлення занадто довге, його ділять і шифрують окремо. Покладемо *e*, *d*, *n* - цілі позитивні числа, з *{e, n}* в якості ключа шифрування, *{d, n}* - ключа дешифрування, де $n = p * q$.

Тепер ми шифруємо повідомлення, підносячи його до степені *e* по модулю *n*, щоб отримати *C* - шифротекст. Для дешифрування *C* його підносять до степеню *d* по модулю *n*, таким чином отримуючи *M* знову. Так ми отримуємо ці алгоритми шифрування і дешифрування для *E* і *D*:

$$C = E(M) = M^e (\,mod\, n)$$

$$M = D(C) = C^d (\,mod\, n).$$

При цьому розмір інформації зберігається, так як *M* і *C* є цілими числами від 0 до *n - 1*, і через модульну конгруенцію.

Сама генерація ключа шифрування основана перш за все на виборі двох випадкових великих простих чисел p та q. Таким чином формується публічна

степінь $n = p * q$, з якої неможливо виявити p та q і таким чином буде й практично неможливо вивести d з e.

Далі отримуються відповідні d та e. Так d, вибирається випадковим великим цілим числом, яке повинно бути взаємно простим з $(\mathrm{p} - 1) * (q - 1)$, що має задовольняти наступному:

$$\text{НОД}(d, (p - 1) \cdot (q - 1)) = 1 .$$

«НОД» означає найбільший спільний дільник.

Далі потрібно обчислити e з d, p та q, де e мультиплікативне зворотне до d. Це означає, що повинно задовольнятись ствердження $e \cdot d = 1\ (mod\ \varphi(n))$. Де $\varphi(n)$ – функція Ейлера, що дозволяє отримати позитивні цілі числа менші ніж n, які взаємно прості з n. Для простих чисел p, це, очевидно, стає $\varphi(p) = p - 1$. Для n, з елементарних властивостей функції Ейлера отримуємо, що

$$\varphi(n) = \varphi(p) * \varphi(q) = (p - 1) * (q - 1) = n - (p + q) + 1.$$

З цього рівняння можна підставити $\varphi(n)$ в рівняння $e \cdot d = 1\ (mod\ \varphi(n))$ та отримати: $e \cdot d = k * \varphi(n) + 1$, для будь-якого цілого k.

За законами модульної арифметики, мультиплікативна інверсія a по модулю m, існує тоді і тільки тоді, a та m взаємно прості. Дійсно, так як d, і $\varphi(n)$ взаємно прості, d має мультиплікативне зворотне e в колі цілих чисел по модулю $\varphi(n)$.

До сих пір, однозначно наступне:

$$D\big(E(M)\big) \equiv \big(E(M)\big)^d \equiv (M^e)^d \ (mod\ n) = M^{e*d} \ (mod\ n)$$
$$E\big(D(M)\big) \equiv \big(D(M)\big)^e \equiv (M^d)^e \ (mod\ n) = M^{e*d} \ (mod\ n)$$

Крім того, так як $e \cdot d = k * \varphi(n) + 1$, ми можемо підставити в наведені вище рівняння і отримати

$$(M^e)^d \equiv M^{k*\varphi(n)+1}.$$

Очікується, що це буде рівне M. Це доводиться використанням важливої особливості Ейлера і Ферма: для будь-якого цілого числа M взаємно простого до n, ми маємо

$$M^{\varphi(n)} \equiv 1 \ (mod\, n)$$

Так як раніше було зазначено, що $0 \leq M < n$, маємо, що M не буде взаємно простим до n, якщо і тільки якщо M рівне p або q, з цілих чисел в цьому інтервалі [10]. Таким чином, шанс, що M опиниться рівним p або q такого ж порядку величина, що і $2 / n$. Це означає, що M є майже безумовно, взаємно простим з n, отже, рівняння $M^{\varphi(n)} \equiv 1 \ (mod\, n)$ має місце і, використовуючи його, ми оцінюємо:

$(M^e)^{\,d} = M^{\,k*\varphi(n)+1} = (M^{\varphi(n)})^k M = 1^k\, M \ \ (mod\, n) = M$.

Це працює для всіх M при цьому задовольняється $(\mathrm{E}\,(\mathrm{M})) = \mathrm{M}$ та $\mathrm{E}\,(D\,(M)) = \mathrm{M}$ для всіх $0 \leq M < n$. Тому E та D є зворотними перетвореннями.

2.1.5 Алгоритм

RSA для обчислення $M^e \ (mod\, n)$ потребує не більше $2 * \log_2(e)$ операцій множення та $2 * \log_2(e)$ операцій ділення, якщо слідувати алгоритму нижче. Даний показник визначає швидкість, а значить і ефективність шифрування. Так виконується піднесення у степінь повторенням піднесення у квадрат та діленням:

1. Нехай $e_k e_{k-1} \ldots e_1 e_0$ бінарне представлення e.
2. Визначити змінну $C = 1$.
3. Повторити кроки 3а і 3б для $i = k, k - 1, \ldots, 0$:

   3а. C присвоїти залишок від ділення C^2 на n.

   3б. Якщо $e_i = 1$, то покласти C рівним залишку від ділення $C * M$ на n.

4. Отримуємо C – зашифроване повідомлення M.

Час шифрування блоку збільшується не швидше, ніж квадрат числа цифр в n.

Число d вибирається взаємно простим до $\varphi(n)$; будь-яке просте число більше за $\max(q,p)$ підходить. Так як множина простих чисел нескінченно велика, вважається, що d не може буде знайдене прямим пошуком.

Для знаходження e використовуються алгоритм Евкліда для розрахунку найбільшого спільного дільника $\varphi(n)$ та d.

Спочатку обчислюється ряд x_1, x_2, x_3, ..., де $x_0 \equiv \varphi(n)$, $x_1 = d, \ldots, x_{i+1} \equiv x_{i-1} \, (mod \, x_i)$, до тих пір, поки не буде знайдено $x_k = 0$. Тоді $\gcd(x_0, x_1) = x_{k-1}$. Далі знаходяться числа a_i та b_i, такі, що $x_i = a_i * x_0 + b_i * x_1$. Якщо $x_{k-1} = 1$ тоді b_{k-1} мультиплікативне зворотне до $x_1 \, (mod \, n)$, а саме e. Це може бути швидко обчислено, так як $k < 2 \log_2 n$. Так як труднощі в обчислюванні складної модульної арифметики частково вносить свій внесок в складність атаки RSA, це являється перевагою. Тому, якщо $e < \log_2 n$, знаходиться інше e, що не настільки мале, щоб зашифроване повідомлення зазнало зниження по модулю n.

2.1.6 Китайська теорема про залишки

Оскільки генерація ключів використовується набагато рідше за шифрування, дешифрування, створення та перевірку підписів, задача обчислення $a = b^c mod \, n$ являється основним обчислювально-складним моментом. Вирішується вона алгоритмом швидко піднесення в степінь і таким чином витрачає $O(ln \, e)$ операцій множення по модулю.

Для аналізу часу виконання операцій з приватним та відкритим ключами, візьмемо $\{d, n\}$ та $\{e, n\}$, які задовольняють умовам : $log_2 e = O(1), log_2 d \leq O(\beta)$. Тоді при їх використанні виконується відповідно $O(1)$ та $O(\beta)$ операцій множення по модулю.

Таким чином час виконання тим більший, чим більше одиниць у двійковому представленні відкритої експоненти. По евристичний оцінкам довжина секретної експоненти d нетривіальним чином пов’язана з відкритою e

та модулем n. Тому дешифровка повільніша за шифрування, а перевірка цифрового підпису швидша за створення [11].

При дешифрування та підписуванні повідомлення алгоритмом RSA показник обчислювальної степені буде достатньо великим числом (близько 1000 біт). Таким чином, потрібен алгоритм, що скоротить кількість операцій. Так як числа p та q в розкладі $N = p * q$ відомі шифрувальнику повідомлення, то можна обчислити:

$$m_p = C^d \, mod \, p = C^{d \, mod \, p-1} \, mod \, p$$

$$m_q = C^d \, mod \, q = C^{d \, mod \, q-1} \, mod \, q$$

Оскільки p та q – числа порядку 2^{512} на ці дії потрібно буде зробити два піднесення у степінь з показником у 512 біт по модулю 512-бітового числа. Це набагато швидше ніж одне піднесення у степінь з 1024-бітним показником по модулю 1024-бітного числа. В кінці потрібно буде лише відновити повідомлення m використовуючи m_q та m_p. Це легко зробити за допомогою китайської теореми про залишки. [12]

Теоретично вважається, що дешифрування з використанням CRT допомагає пришвидшити процес у чотири рази. Середній час дешифрування нормального методу близько 0.157 секунд, а з використанням китайської теореми становить близько 0.046 секунд, що дає приріст по швидкості приблизно у 3.4 рази.

2.1.7 Оцінка безпеки алгоритму

Складність атаки на RSA зазвичай пов’язують з важкістю факторизації числа n. Таку задачу вважають невиправдано важкою, через відсутність алгоритму, що зможе виконати її з числами порядку 200 за прийнятний проміжок часу. Саме це забезпечує алгоритму RSA статус надійного.

Припускається, що кількість операцій та час за який може бути виконана факторизація відповідає даним з Таблиці 2.1.

Таблиця 2.1 – Складність факторизації чисел заданої розрядності

Розрядність	Кількість операцій	Час
50	1.4×10^{10}	3.9 годин
75	9.0×10^{12}	104 дні
100	2.3×10^{15}	74 роки
200	1.2×10^{23}	3.8×10^{9} років
300	1.5×10^{29}	4.9×10^{15} років
500	1.3×10^{39}	4.2×10^{25} років

Таким чином рекомендована розрядність для *n* складає більше 200, іншими словами - використання ключа довжиною 2048 біт або більш. Слід також враховувати, що більша довжина ключа веде до зменшення швидкості роботи алгоритму, тому при необхідності її зменшують. Це залежить від специфіки задачі та потреб в безпеці та швидкодії , які висуваються до алгоритму. Також якщо використовувати китайську теорему про залишки для пришвидшення алгоритму можна зберегти надійність алгоритму на високому рівні. Крім того пришвидшуючи алгоритм китайською теоремою про залишки ускладнюються часові атаки на нього.

2.2 Аналіз по стороннім каналам та його види

Враховуючи складність математичного апарату алгоритмів шифрування, які на сьогодні являються стандартом в сфері інформаційної безпеки, зловмисники знайшли інший підхід до атак на криптосистеми. В їх основі лежить збір та аналіз інформації по так званим, стороннім каналам.

Сторонні канали являють собою варіант класичної проблеми прихованого каналу. Приховані канали включають в себе два або більше процесів, що співпрацюють для зв'язку через загальний ресурс, на який вони обидва мають вплив. Зловмисники можуть експлуатувати ці канали для обходу захисту операційної системи, такого як обов'язковий контроль доступу, який призначений для відокремлення процесів. Наприклад, один процес може

виділяти пам'ять в той час як інший вимірює обсяг вільної пам'яті. За допомогою повторення такої поведінки, перший процес може повільно передавати інформацію другому. Відношення сигнал/шуму каналу оцінює його якість. Наприклад, виділення пам'яті непов'язаними процесами може спотворити результати деяких вимірювань, тому особливо зайнята система може мати низьке відношення сигнал/шуму. В цьому випадку можуть допомогти методи корекції помилок.

Сторонні канали виникають тому, що обчислення відбувається в неідеальній системі, що складається з транзисторів, дротів, джерел живлення, пам'яті та периферійних пристроїв. Кожен компонент має характеристики, які змінюються в залежності від команди та даних, що обробляються. Коли ці дані вимірюються зловмисником – сторонній канал присутній. Атаки, в основі яких лежить аналіз подібної інформації мають назву Side channel attacks (SCA) [13].

Основна ідея SCA - це подивитися на те, як криптографічні алгоритми були реалізовані, а не на алгоритми як такі. Звичайний крипто аналіз розглядає криптографічні алгоритми, як чисто математичні об’єкти. SCA отримують для аналізу інформацію зі сторонніх каналів, які несуть в собі особливості реалізації алгоритмів. Закодований функціонувати належним чином алгоритм не повинен розкривати дані про використання секретного ключа, навіть якщо хтось може спостерігати за протіканням його роботи. Такі атаки працюють через кореляцію між фізичними характеристиками виміряними під час обчислень (такі як споживання енергії, час обчислень, електромагнітне випромінювання та інші) та внутрішнім станом процесів в пристрої, які в свою чергу напряму пов’язані з приватним ключем. Такі атаки набагато ефективніші за традиційний математичний аналіз, та їх набагато простіше здійснити [14].

Традиційно, безпечні алгоритми шифрування гарантують захищеність від спостерігача, котрий має доступ до «чорного ящика» (Рисунок 2.1), що

реалізує шифрування. Тим не менш такі моделі не завжди адекватно спроектовані. Зокрема, безпеку цих алгоритмів може бути повністю обійдена атаками, які намагаються підробити секретний ключ.

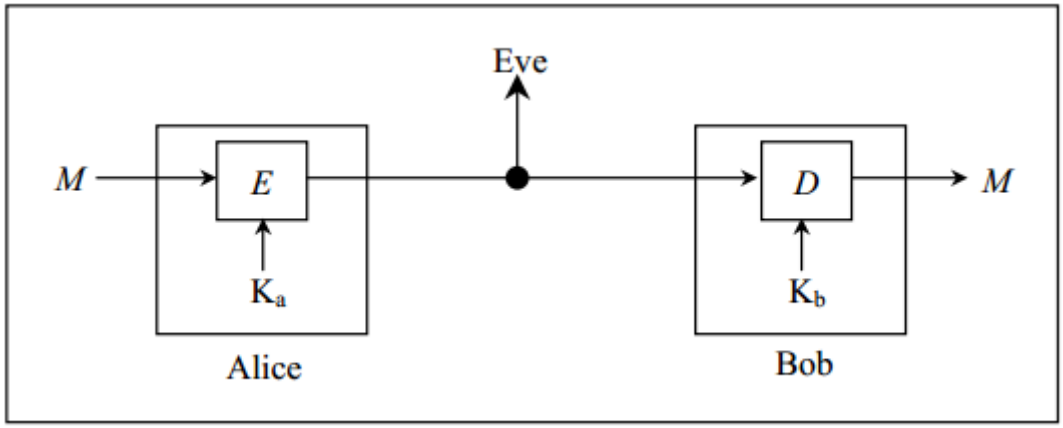


Рисунок 2.1 – Традиційна криптографічна модель

Використовуючи можливості SCA, зловмисник може спостерігати та виміряти показники системи, а потім зібрану інформацію спрямувати на розкриття секретного ключа [15]. Втручаючись таким чином в роботи криптосистеми, їїх модель для зловмисника набуває вигляду, як на Рисунку 2.2.

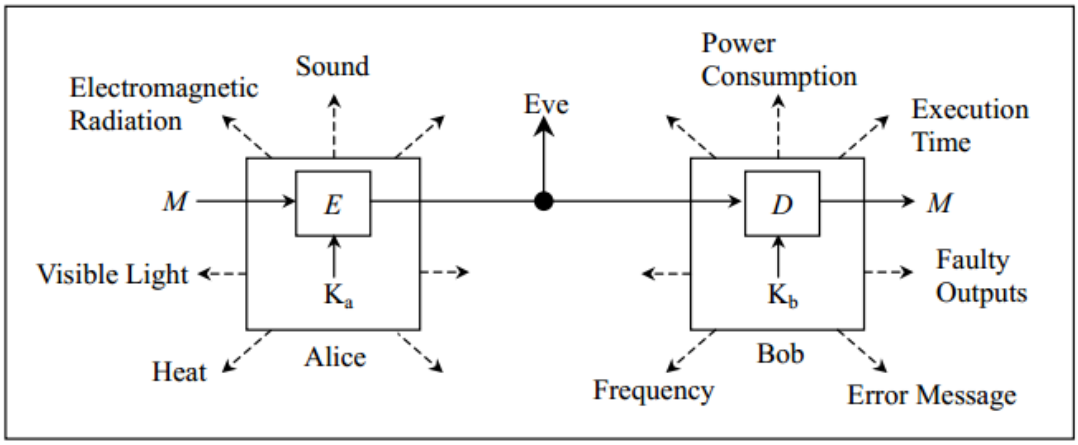


Рисунок 2.2 – Криптографічна модель, що включає сторонні канали

2.2.1 Часовий аналіз

Одним з найбільш ранніх і найбільш легко зрозумілих атак з боку каналу є атака синхронізації.

Часова атака має місце, коли з витоку інформації по сторонньому каналу отримують шляхом спостереження кількості часу, що потрібен на виконання операція. Приклад цього можна знайти з простої низки порівнянь, отриманої з використання роботи функції перевірки паролю. Система завантажує обидва рядки в пам'ять і послідовно порівнює кожен байт. Як тільки порівняння не вдається, цикл завершується і функція повертає результат, що рядки не збігаються (або невірний пароль). Однак, якщо кожне порівняння вірне до кінця рядка, то функція повертає результат, що рядки збігаються (або доступ надано). Число порівнянь, що виконує функція, перед тим як повертає результат безпосередньо пов'язане з числом співпадаючих байт в рядках. Тепер припустимо, що виконання кожної операції порівняння байтів займає 1 мікросекунду. Порівняння рядків, в яких перші шість байт співпадають займе на 4 мікросекунди більше, ніж для рядків з однаковими двома байтами. Перевірка паролю, що працює таким чином (з використанням стандартного порівняння строк) гарантовано уразлива до такої простої часової атаки, так як зловмисник використовуючи прямий перебір (brute-force) володіє інформацією про свій прогрес, що значно скорочує множину для пошуку пароля.

Пол Кохер перший опублікував такі часові атаки на криптосистеми [16]. Кохера основує свою атаку на тому факті, що обчислювально-дорогі криптографічні функції часто виконуються за змінний часу. У найпростішому випадку, він демонструє атаку на бінарному модульному методі піднесення в степінь. Це ітераційний алгоритм, який, в кожній ітерації свого циклу виконує або пропускає операцію по модулю, грунтуючись на значенні кожного біта на вході. Бітове значення, яке призводить до того, виконання модулю займає більше часу, ніж значення, яке пропускає виконання. Таким чином, шляхом

проб і помилок, зловмисник може в кінцевому випадку з'ясувати всі вхідні значення. Кохер продовжує пояснювати, як цей принцип може бути застосований до різних криптосистем, наприклад, таких як RSA.

Ідеї Кохера використав Дем та інші [17], щоб створити робочу атаку на реалізацію RSA для смарт-карт, що спричинила модифікацію цієї реалізації. Слід зазначити, що атака провалиться проти реалізацій RSA з використанням китайської теореми про залишки, але Шиндлер в [18] показав часову атаку, яка вирішує цю проблему і ще більш ефективна, ніж оригінальні атаки.

2.2.2 Аналіз потужності

Атаки основані на аналізі потужності є ще одним засобом обробки інформації, отриманої зі сторонніх каналів. Аналіз потужності спирається на той факт, що струм тече через транзисторні переходи, коли даний транзистор знаходиться у включеному стані. Таким чином, параметри роботи пристрою можна спостерігати через зміни в загальному спожитому струмі: кожен транзистор у відкритому стані збільшує необхідний струм, а транзистори в закритому стані мають протилежні ефект. Такі невеликі зміни в спожитому струмі створюють детальний опис низького рівня даних, інструкції та процесів виконання, що відбуваються всередині пристрою. Крім того, слідкуючи за тим як різні модулі мікроконтролера вмикаються та вимикаються, побачені закономірності і зміни в споживаної потужності для системи в цілому показують великомасштабні операції у часі [13].

Аналіз потужності вимагає вимірювання струму, спожитого пристроєм. Це досягається шляхом розміщення невеликого опору резистора відповідно до вхідної потужності пристрою. Падіння напруги на резисторі потім вимірюється за допомогою традиційного осцилографа і використовується закон Ома для перетворення цієї напруги в струм ($I = \Delta V/R$).

Атаки, що використовують цю властивість, грунтуючись тільки на замірі одного циклу потужності називають простий аналіз потужності (SPA). Це метод, який включає в себе безпосередньо інтерпретацію вимірювань споживаної потужності, зібраних в ході криптографічних операцій. У SPA атак, споживана потужність пристрою, в основному, аналізується по осі часу. Зловмисник намагається знайти шаблони чи намагається зіставити шаблони в одному сліді.

В випадку з алгоритмом RSA, що реалізує схему цифрових підписів аналізують модульне піднесення у степінь. Припустимо, що підпис s генерується з повідомлення m обчисленням $s = \mu(m)^d \, mod \, n$, де d – це приватний ключ, n – добуток двох великих простих чисел, а μ – відповідна функція відступу. Підпис звіряється шляхом перевірки правильності рівності $\mu(m) = s^e \, mod \, n.$ Один з більш розповсюджених алгоритмів піднесення у степінь це алгоритм піднесення у квадрат та множення, де степінь e читаються побітово зліва направо. Починаючи з регістра встановленого в 1, операція піднесення у квадрат виконується коли зустрічається біт рівний 0, а на нею слідує операція множення (на значення рівне піднесенню в степінь e) якщо біт рівний 1 [20]. На рисунку 2.3 представлене споживання енергії мікропроцесором при виконанні описаного вище алгоритму.

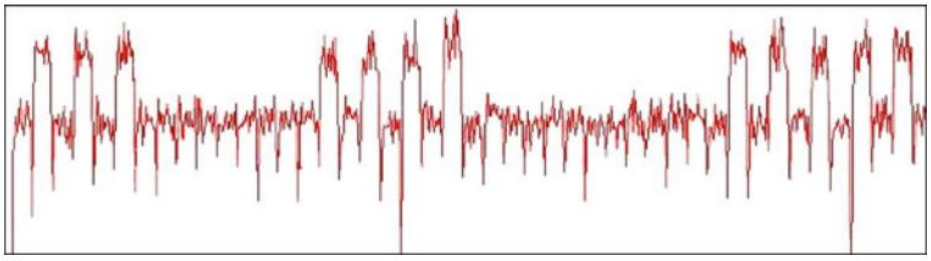


Рисунок 2.3 – Спожита електроенергія при піднесені у степінь

В спожитій електроенергії можна побачити серію операцій, що відокремлені один від одного спадними піками. Зі співвідношення операцій, визначених алгоритмом, можна зробити висновок, що низьке

енергоспоживання відповідає операції піднесення у квадрат, а більш високі затрати потужності – множенню. Якщо провести аналогію між отриманим сигналом і залежність вхідного біта та відповідної операції, можна визначити отримані результати, як реакцію на експоненту :

11110000000011110000000000011111.

На відміну від SPA атак, диференціальні атаки потужності (DPA) вимагають великої кількості записів сигналів. Основна перевага DPA атак в порівнянні з SPA є те, що не потрібно особливих знань про пристрій, що реалізує в собі криптосистему. Насправді, як правило, досить знати криптографічний алгоритм, який виконується пристроєм. Ще одна важлива відмінність між цими двома видами атак є те, що записані сигнали аналізуються по-іншому.

Метою DPA атак є виявлення секретних ключів криптографічних пристроїв на основі великої кількості сигналів енергетичного споживання, які були зареєстровані в той час як пристрій зашифрував або розшифрував різні блоки даних. На відміну від SPA атак, в даних атаках є загальна стратегія, що використовується в усіх DPA атаках. Ця стратегія складається з п’ятьох кроків.

1. *Вибір проміжного результати для обчислювального алгоритму*. Цей проміжний результат повинен бути функцією $f(d,k)$, де d це відоме, не постійне значення, а k –невелика частина ключа. Проміжний результат, що задовольняє цим умовам, може бути використаний для виявлення k. В більшості сценаріїв атак, d це повідомлення або шифротекст.
2. *Вимірювання спожитої електроенергії.* Другий крок DPA атак – виміряти споживання під час виконання криптосистемою шифрування чи дешифрування D різних блоків даних. Для кожного з цих прогонів шифрування або дешифрування зловмисник повинен знати відповідне значення даних d, яке використовувалось в обчисленнях проміжного

результату в кроці 1. Ці відомі дані записуються у вигляді вектора $d = (d_1, \dots, d_D)'$, де d_i позначає дані в i-тому прогоні шифрування чи дешифрування. Впродовж кожного з прогонів зловмисник записує сигнал споживання для кожного блоку даних, якому відповідає $t'_i = (t_{i,1}, \dots, t_{i,T})$, де T – довжина прогону. Всі прогони можуть бути представлені у вигляді матриці розмірністю $D \times T$. Також для DPA атаку дуже важливо правильно вирівняти отримані сигнали, так щоб значення спожитої енергії для кожної колонки t_j в матриці T були відповідними до тих самих операцій. Для того щоб отримати вирівняну спожиту потужність, ініціюючий сигнал для осцилографа повинен бути сформований таким чином, щоб осцилограф фіксував споживання енергії точно тих же послідовностей операцій під час кожного прогону шифрування або дешифрування.

3. *Розрахунок гіпотетичних проміжних значень.* Наступне – обчислити гіпотетичне проміжне значення для всіх можливих $k = (k_1, \dots, k_K)$, де K позначає максимальну кількість можливих виборів. В контексті DPA атак елементи цього вектора, зазвичай сприймаються як гіпотетичні ключі. Маючи вектор даних d та вектор гіпотетичних ключів k, зловмисник може легко обчислити гіпотетичні проміжні значення $f(d, k)$ для всіх прогонів шифрування D та для всіх гіпотетичних ключів K. Результатом обчислення $v_{i,j} = f(d_i, k_j)$ буде матриця V розміром $D \times K$ (Рисунок 2.4). Колонка j при цьому містить проміжний результат при гіпотетичному ключі k_j. Зрозуміло, що значення, яке насправді використовую пристрій – це елемент вектору k. Це й є ключ пристрою, який позначимо k_{ck}. Таким чином мета DPA знайти яка з колонок матриці V обробляється під час виконання шифрування чи дешифрування.

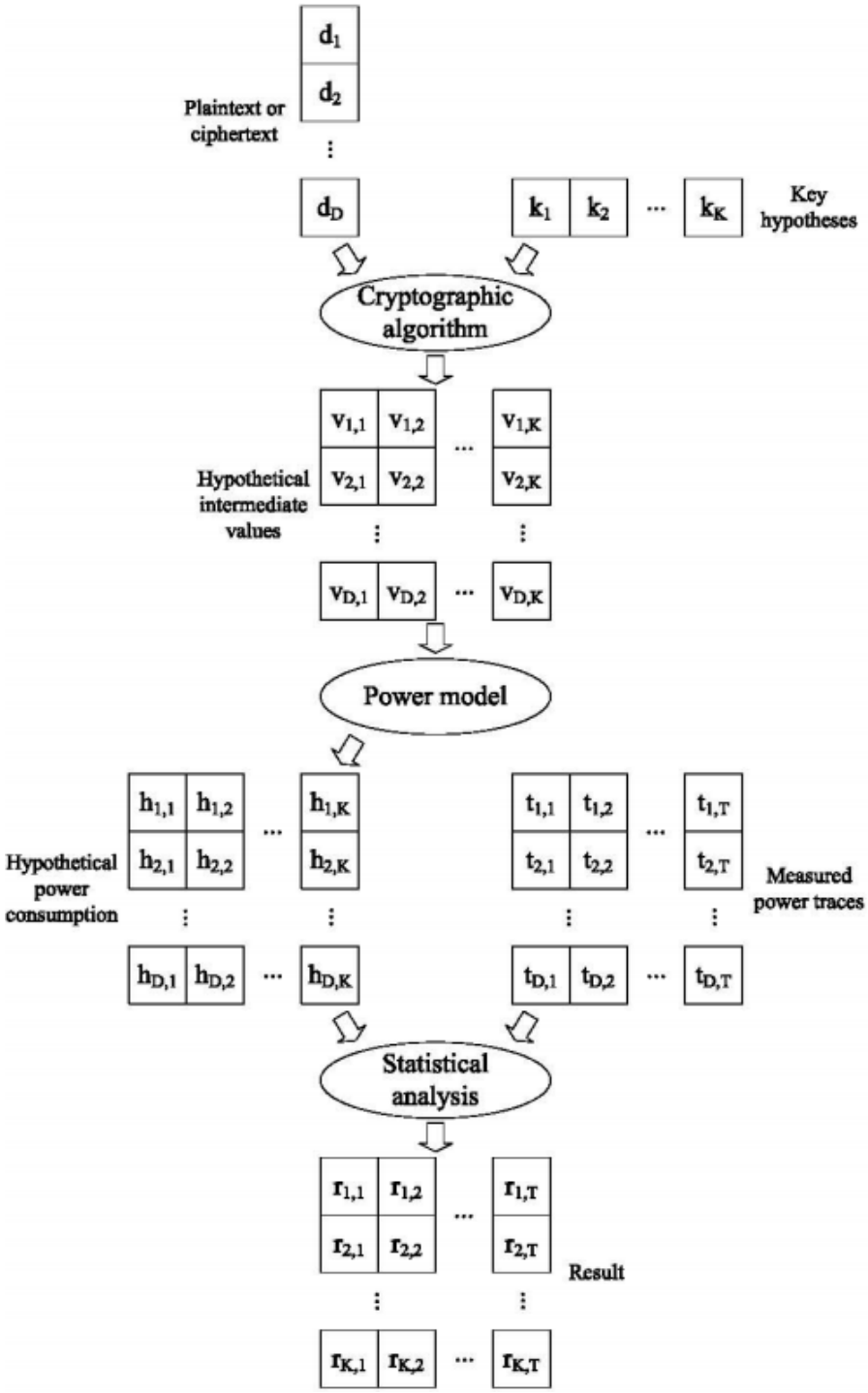


Рисунок 2.4 – Кроки 3-5 DPA атаки

4. *Відображення проміжних значень на значення спожитої енергії.* Наступний крок в DPA відобразити гіпотетичні проміжні значення V в матрицю H гіпотетичних значення споживаної енергії (Рисунок 2.4). Для цього гіпотетичні проміжні значення $v_{i,j}$ симулюються з метою отримати гіпотетичне споживання $h_{i,j}$. Успіх результату симуляції

залежить від знань про пристрій. Найчастіше для цього використовують модель Хемінга.

5. *Порівняння гіпотетичних значень споживання з заміряними.* На останньому кроці виконується порівняння колонок матриці *H* та *T* з результуючою матрицею *R* (Рисунок 2.4). Таким чином, зловмисник може знайти вірний ключ, що використовує пристрій.

2.2.3 Аналіз помилок

Більшість пристроїв, що виконують різні криптографічні операції, як правило, мають надійно працювати, коли ми використовуємо їх, щоб ми не могли б навіть думати, що безпека таких операцій залежить від надійності пристроїв, що реалізують їх. Незважаючи на це припущення, було продемонстровано, що апаратні помилки і помилки, що виникають в процесі роботи криптографічного модуля насправді можуть серйозно вплинути на безпеку. Ця дефектна поведінка та вихідні дані можуть також стати важливою інформацією зі стороннього каналу, і навіть значно збільшити вразливість шифрування до крипто аналізу. Помилки представляють практичні і ефективні атаки проти криптографічних пристроїв, таких як смарт-карти [19].

Є два основних види помилок зі сторонніх каналів. Перші з них це канали, які спричинені обчислювальними помилками, що виникають в процесі обчислень криптографічного модуля, що атакується. Ці помилки можуть бути випадковими або навмисно, викликаними, наприклад, за допомогою точного маніпулювання напругою. Маючи можливість спричинити обчислювальні помилки, цей вид атаки може бути використаний практично на кожному виді криптографічного механізму, і він вважається одним з найефективніших атак з усіх атак по стороннім каналам [23]. Другі види помилок зі сторонніх каналів є ті, які спричиняються шляхом посилки навмисно пошкоджених вхідних даних для модуля, що атакується. Для модуля, це означає нестандартну ситуацію, яка повинна бути оброблена спеціальним чином. Зазвичай модуль повинен

використовувати повідомлення про помилку, що інформує користувача (модуль навряд чи може знати, чи це звичайний користувач чи зловмисник), що обчислення було припинено в зв'язку з якими-небудь причинами [19].

2.2.4 Електромагнітний аналіз

Електромагнітний аналіз дає ще один засіб використання інформації стороннього каналу для атаки. Замість того, щоб захопити енергоспоживання даного пристрою, вимірюються електромагнітні (ЕМ) еманації. Комплементарні напівпровідникові пристрої з оксиду металу (КМОП), які включають в себе більшість напівпровідникових приладів сьогодні, споживають потужність під час переходу затворів від високих до низьких рівнів. Крім того, акт перемикання затвора викликає крихітне коротке замикання і невеликий сплеск споживання струму як сигнал поширюється через транзистор [15]. Всі ці зміни в потоці потужності змінюють електромагнітне поле, що оточує пристрій, і ці зміни можуть бути зафіксовані за допомогою спеціального зонда.

Збір ЕМ даних вимагає близьке розміщення зонда, який містить просту дротову котушку. Цей зонд розміщується дуже близько до пристрою, що аналізується. Поточні рухи всередині пристрою викликають малі струми в котушці, які потім посилюються приєднаним малошумним підсилювачем (МШУ) і перехоплюються осцилографом. Ці отримані дані аналізуються в основному так само, як і в атаках на основі аналізу потужності. Електромагнітний аналіз має деякі переваги в порівнянні з аналізом потужності [15]. На відміну від DPA, це не агресивна атака, що усуває необхідність модифікації цілі. По-друге, підхід з використанням рухомого зонда випливає в здатність виконувати локалізовані перехвати. Іншими словами, якщо центральний процесор, як компонент SoC, має витік більшої частини інформації, зонд розташовується безпосередньо над областю цієї деталі для отримання сильнішого сигналу і менших шумів. Аналіз потужності, з іншого боку, обмежений сукупністю споживаної потужності всього пристрою. Нарешті,

електромагнітний аналіз (ЕМА) дозволяє спостерігати цикли зарядки і розрядки воріт дискретно, забезпечуючи більш детальну інформації про переходи кожного затвору, ніж аналіз потужності [41].

2.3 Методи протидії крипто аналізу

До сих пір, існує багато стратегій (як апаратних так і програмних засобів) які пропонують методи протидії атакам з боку сторонніх каналів, серед яких є деякі загальні стратегії:

- де-корелювати вихідні результати на окремі прогони (наприклад шляхом введення довільних часових зсувів та станів очікування, вставлення фіктивних інструкцій, виконання операцій в довільному порядку і т.д.);
- замінити критичні асемблерні інструкції на інші, «споживчі сліди» яких важко аналізувати, чи перепроектувати критичну схему, яка виконує арифметичні операції або перезаписи в пам’яті;
- зробити алгоритмічні зміни в криптографічних примітивах так, що атаки стануть доказово не ефективними на досліджуваній реалізації, наприклад, маскувати дані та ключ довільно згенерованою маскою для кожного циклу шифрування.

Було показано, що з усіх цих видів протидій, алгоритмічні техніки є найбільш універсальними, все-проникними та мабуть найпотужнішими. Крім того, у багатьох випадках, вони є найдешевшими у втіленні. Програмні заходи протидії включають впровадження фіктивних інструкцій, рандомізацію послідовності виконання інструкцій, балансування ваг Хеммінга внутрішніх даних та розщеплення біт. На апаратному рівні контрзаходи зазвичай включають рандомізацію часу, споживання енергії чи її компенсація, рандомізація виконання набору інструкцій та/чи використання регістрів. Тим не менш, ефект таких контрзаходів може бути зменшений за допомогою різних технік обробки сигналів [32].

Програмна протидія атакам по стороннім каналам значно ускладнює виконання криптографічних алгоритмів, коли справа стосується операцій з

пам’ятю чи часу виконання чи обох факторів. Одна з проблем - це досягнення безпечної імплементації з мінімальними додатковими витратами, наскільки це можливо.

Вибір відповідного рівня протидії контрзаходів може залежати від значення даних та можливостей зловмисника (наприклад, його знання про пристрій і ресурси та інше).

Оцінка рівня захисту повинна бути проведена принаймні з наступних трьох кутів: можливості зловмисника (у тому числі його знань, ресурсів і навичок Етал.), можливості атак (які тісно пов'язані з їх реальним станом) та ефективність контрзаходів. Виявляється, що поєднання апаратних і програмних контрзаходи дає дуже гарне співвідношення безпеки / вартості.

Ми можемо знайти наступні проблеми та пов’язані дискусії в відкритій літературі: атаки, контрзаходи (такі як програмне забезпечення і апаратні засоби) та теоретичні моделі.

2.3.1 Рандомізація

Найбільш загальний спосіб, щоб протистояти атакам SCA, це рандомізувати дані, які можуть витекти через різні сторонні канали, такі як споживання потужності, електромагнітне випромінювання, або час виконання.

Проблема полягає в тому, що, щоб гарантувати те, що зловмисник може отримати тільки випадкову інформацію, і, отже, не може отримати будь-які корисні знання про фактичні початкові і / або проміжні дані, що беруть участь в обчисленнях.

У разі криптосистем з еліптичними кривими, метод рандомізованих проективних координат є практичним контрзаходом для SCA атак, в яких атакуючий не може передбачити виникнення певного значення, оскільки координати були довільними. Також запропоновано SCA-стійкий метод скалярного множення, якому дозволено приймати будь-яку кількість попередньо обчислених точок. Така схема по суті має намір захистити від простого аналізу споживання, а не диференціального [24].

Стандартно DPA використовує функцію кореляції, яка може розрізняти, чи пов'язаний конкретний біт зі спостережуваними обчисленнями. Для того, щоб протистояти DPA, ми повинні рандомізувати параметри еліптичних кривих. Є три стандартних методи рандомізації зазвичай доступні сьогодні:

- базова точка маскується довільною точкою;
- секретний скаляр рандомізується з множником порядку кривої;
- базова точка рандомізується в проективних координатах (або Якобіанових координатах).

2.3.2 Сліпота

Сліпота – це оригінальне поняття в криптографії, що дозволяє клієнту мати постачальника, що обчислює математичну функцію $y = f(x)$, де клієнт забезпечує вхідні дані x і отримує відповідні вихідні y, але провайдер зможе дізнатись ні x ні y. Ця концепція корисна, якщо клієнт не може обчислити математичну функцію f сам по собі, наприклад, тому що провайдер користується додатковими приватними даними для ефективного обчислення функції.

Вперше метод був запропонував Чаум як частину підпису Чаума [22, 23]. Він заснований на гомоморфних властивостях методу цифрового підпису RSA. Техніки осліплення також є найбільш ефективними контрзаходами проти віддаленого часового аналізу веб-серверів та проти аналізу енергій споживання чи часового аналізу апаратних криптографічних модулів.

2.3.3 Уникнення умовних переходів та секретних проміжних даних

Вважається, що уникнення процедур, що використовують проміжні секрети чи ключі для умовних переходів замаскує багато інформації, що містять сторонні канали.

Програмна реалізація критичного коду не повинна містити операції відгалуження. Також вона не повинна містити умовно виконувані вирази, такі як умову if. Обчислення повинні виконуватися з використанням функцій, які утилізують елементарні операції (так як І, АБО та сума по модулю два) і не використовують відгалуження чи умовне виконання частин коду.

Така протидія може значно ускладнити намагання зловмисника вгадати вхідні дані та значення ключів використовуючи вимірювання часу чи спожитої енергії. Умовне виконання коду, яке залежить від вхідних даних та ключа, може легко розкрити властивості цих даних, якщо зловмисник вимірює час та споживання при виконанні саме цієї дії. Коли всі строчки коду завжди виконуються незалежно від вхідних даних чи бітів ключа, час та енергія затрачена на виконання операції не несуть інформацію про дані і не залежать від них, таким чином їх характеристики не розкриваються.

Ця протидія допомагає запобігти як всім типам часового аналізу на асиметричні шифри, так і деяким атакам, основаним на даних про спожиту енергію.

2.3.4 Додавання затримок

Найочевиднішою протидією часовому аналізу – зробити так, щоб всі операції займали однаковий час. Нажаль найчастіше це дуже складно. Якщо використовувати таймер для затримки повернення результату до заданого часу, такі фактори, як відклик системи на запити чи споживання енергії можуть до сих пір виказувати момент завершення операції і таким чином це все ще не змінює ситуацію [35].

Також, операції, що виконуються за фіксований проміжок часу є досить повільними, а оптимізація не може біти використана, так як всі операції все рівно повинні мати однаковий час виконання з найповільнішою.

Коли додаються випадкові затримки, вони також підвищують кількість необхідних шифротекстів, які зловмисник зможе компенсувати збиранням та аналізом більшої кількості заміряних даних. Кількість зразків повинна бути збільшена приблизно на квадрат синхронізації шуму. Таким чином, довільні затримки можуть хіба що зробити часовий аналіз більш складним, але не неможливим.

2.3.5 Вирівнювання часу множення та зведення у квадрат

Час, що потрібен модулю для виконання піднесення у степінь та множення, повинен бути однаковий. Раніше вже згадувалось, що визначення яка саме операція має бути наступною напряму пов’язана з вхідними бітами ключа, що й може допомогти його викрити. Якщо часовий аналіз буде направлений на спробу виявити яка операція має місце в залежності від часу її виконання, дана протидія перешкоджатиме цьому. Звичайно це не зможете протистояти аналізу по споживанню енергії [34].

Вирівнювання може бути втілено шлях постійного виконання обох операцій (множення та піднесення у степінь), незважаючи на те, яка операція повинна бути виконана насправді. На кожному етапі, коли одна з операцій повинна бути виконана, виконуються обидві, а результат маскуючої операції повинен бути непомітно проігнорований.

Така протидія результативна проти часового аналізу піднесення у степінь в рамках асиметричного шифрування, що є предметом багатьох розповсюджених атак.

2.3.6 Балансування спожитої потужності

Якщо можливо, обов’язково слід застосовувати техніки для балансування напруги. Додаються фальшиві регістри та вентилі, що виконують незначущі операції для збалансування споживання енергії до деякого константного значення. Кожен раз коли операція виконується апаратно, додаткові операції

повинні бути запущені на фальшивих елементах для впевненості, що загальне споживання енергії модуля залишиться врівноваженим до деякої вищої величини [39, 40].

Забезпечуючи постійне значення споживання в незалежності від вхідних бітів ключа допомагає запобігти всім видам атак по споживанню, й простим й диференційованим.

2.3.7 Зниження розміру сигналу

Існує підхід для попередження диференційного аналізу по споживанню, в основі якого лежить зниження розміру сигналу шляхом використання константних шляхів виконання коду, вибору операцій, які зливають менше інформації по спожитій енергії, балансування вагів Хеммінга та постійних переходів чи шляхом фізичного захист пристрою від доступу до нього зловмисника [25].

Нажаль такі підходи до зменшення розміру сигналу, не можуть звести його до нуля, й зловмисник з дуже великою кількість замірів все ще зможе провести диференційний аналіз.

2.3.8 Додавання шуму

Також підхід до захисту від DPA включає додавання шуму в вимірювання спожитої енергії. Як зменшення розміру сигналу, додавання шумів збільшує кількість замірів, що необхідні для проведення успішної атаки, і ймовірно до невиправдано великих значень. До того ж, час виконання та порядок може бути рандомізований для створення такого ж ефекту [25]. Як і в минулому підході, один лише шум лише підвищує складність атаки збільшуючи кількість необхідних замірів, тим не менш, якщо це збільшення настільки велике, що атака не буде доцільною, така протидія також може мати місце.

Протидія диференційному аналізу шляхом додавання шуму може бути втілена запуском довільних обчислень, які збільшать рівень шуму достатньо для того, щоб зробити невиявними зміщення піків при DPA [26].

2.3.9 Фізичний захист

На практиці, агресивний фізичний захист пристрою може зробити атаки не ефективними, але вартість на розміри пристрою значно збільшуються, що зазвичай вважають ще більшим недоліком [25].

2.3.10 Модифікація дизайну алгоритму

Вирішальний метод протидії DPA атакам є ре-дизайн криптосистеми враховуючи реалістичні сподівання щодо апаратних засобів, які будуть використовуватися. Нелінійні процедури оновлення ключа можуть бути використані для гарантування відсутності кореляції між електричними рештками та взаємодіями. Простим прикладом може бути хешування 160-бітного ключа алгоритмом SHA перед використання його як ключа. Це може ефективно зруйнувати частину інформації, що зловмисник може зібрати про ключ.

Аналогічним чином, агресивне використання експоненти і модифікація процесів, що стосуються модулю в схемах з відкритим ключем можуть бути використані для запобігання накопичення даних шляхом проведення великої кількості замірів зловмисником.

2.3.11 Запуск шифрування двічі

Серед протидій атакам за помилками [24], можливим рішенням може стати запуск модуля шифрування двічі й виведення результату тільки за умови, що вони співпали. Головним недоліком при цьому вважають збільшення часу виконання обчислень, особливо, звертаючи увагу на те, що алгоритм RSA й так повільний. Також цей метод не зможе гарантувати, що помилка не виникне обидва рази, а тому не гарантується повний захист від атак за помилками.

Насправді вони все ще мають місце бути, але для успішного проведення вимагають набагато більшу вибірку.

2.3.12 Апаратне приховання

Інша група протидій впливає на тактовий сигнал. Такі методи випадковим чином змінюють тактовий сигнал для того, щоб зробити вирівнювання потужності складнішим для спостереження. Найбільш часто використовувані методи, щоб маніпулювати тактовим сигналом криптографічних пристроїв наведені нижче [33].

• *Пропуск тактових імпульсів.* Основна ідея цього підходу полягає в тому, щоб вставити щось подібне фільтру на шляху тактового сигналу. Цей фільтр випадковим чином пропускає імпульси тактового сигналу, який забезпечується криптографічним пристроєм. Випадкові числа використовуються для визначення тактових імпульсів, які пропускаються, та які ні.

• *Довільна зміна тактової частоти.* Альтернатива пропуску тактових імпульсів – це генерування сигналу синхронізації зі зміною у випадковому порядку частоти, безпосередньо на криптографічному пристрої. Це може бути, наприклад, зроблено шляхом регулювання частоти внутрішнього генератора на основі випадкового числа.

• *Паралельні годинникові сигнали.* В цьому випадку кілька сигналів синхронізації генеруються на криптографічному пристрої. Вирівнювання операцій криптографічного алгоритму руйнуються випадковим перемикання між годинниковими сигналами.

2.3.13 Маскування

Протидія атакам на основі аналізу потужності на елементарному рівні була одна з перших реакцій напівпровідникової промисловості після публікації цих атак. У науковому співтоваристві, це зайняло набагато більше часу, поки з'явилися перші пропозиції щодо контрзаходів елементарного рівня. В останні

роки кілька пропозицій, щоб протистояти атакам аналізу потужності, були зроблені для логічних рівнів. Багато з цих логічних стилів протидії засновані на концепції приховування [29, 31].

Застосування концепції приховування на елементарному рівні означає, що логіка комірки зі схеми реалізована в такий спосіб, що їх енергоспоживання не залежить від оброблюваних даних і виконуваних операцій. Ця незалежність зазвичай досягається шляхом константного споживання енергії логічних елементів в кожному тактовому циклі для всіх оброблених логічних значень. Константа в кожному тактовому циклі означає, що миттєве споживання енергії в елементі є таке ж саме в кожному такті. Наслідком такої поведінки є те, що логічні елементи завжди споживають максимальну кількість енергії в кожному такті. Загальна споживана потужність криптографічного пристрої постійна в цьому випадку. Таким чином, вона не залежить від оброблюваних даних і виконуваних операцій.

Логічні підходи з постійним споживанням потужності протидіють SPA атакам і DPA атакам. Однак такі логічні втілення часто просто називають DPA стійкістю логічні рівня, тому що протидіяти DPA атакам, як правило, їх основне поле застосування. Логічний підхід з постійним споживанням потужності, як правило, реалізований у вигляді подвійного рейки предзарядки (DRP) логічних елементів.

2.3.14 Багатопотоковість

Враховуючи специфіку реалізації криптосистем на вбудованих пристроях, та їх розповсюдженість саме на такого роду приладах можна використовувати особливості реалізації багатопотоковості на них.

Існують багато класів приладів, виділимо та дослідимо детальніше особливості використання реалізованої на них багатопотоковості до імплементації алгоритму RSA. Таким чином, розглянемо приклади пристроїв,

які реалізують в собі урізану версію операційної системи та ті, що виконують лише чистий покладених у них бінарний код.

1. *Пристрої з урізаною операційною системою.* Розглянемо особливості архітектури плати TM4C1294XL серії Tiva C фірми Texas instruments (Рисунок 2.5).

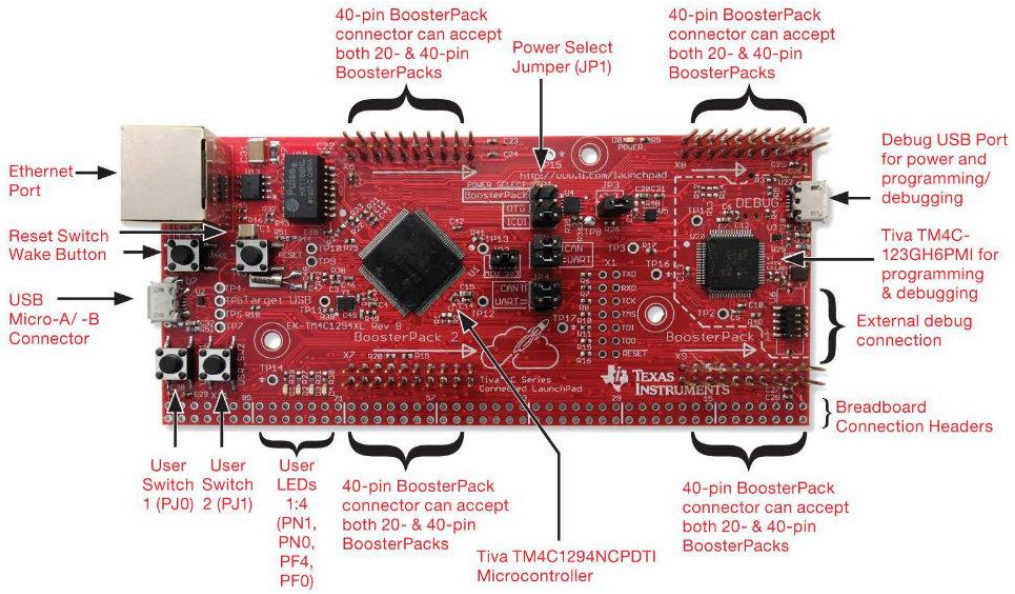


Рисунок 2.5 - Плата TM4C1294XL

В її основі лежить урізана операційна система, що при програмування потребує ініціалізації системного пакету та BIOS. Він працює як нескінченний цикл, що постійно виконує запрограмовані завдання – “Tasks”, які можна побачити нижче на Рисунку 2.6. Всі завдання виконуються одночасно, це може бути використано для розділення алгоритму RSA на декілька потоків. Таким чином, спектральний аналіз спожитої потужності при шифруванні та дешифруванні накладе сигнали кожних завдань один не одне і точне виділення значень біт ключа значно ускладниться. Розподілення на завдання може вестись по принципу потрібної дії, вони програмно реалізуються як одночасно виконувані функції.

```
/* ======== main ======== */
Int main(Int argc, Char* argv[])
{
    Task_Params params;
    Error_Block eb;

    Error_init(&eb);
    Task_Params_init(&params);

    params.instance->name = "myTsk0";
    myTsk0 = Task_create(myTsk0Func, &params, &eb);
    if (myTsk0 == NULL) {
        System_abort("myTsk0 create failed");
    }

    params.instance->name = "myTsk1";
    myTsk1 = Task_create(myTsk1Func, &params, &eb);
    if (myTsk1 == NULL) {
        System_abort("myTsk1 create failed");
    }

    params.instance->name = "myTsk2";
    myTsk2 = Task_create(myTsk2Func, &params, &eb);
    if (myTsk2 == NULL) {
        System_abort("myTsk2 create failed");
    }

    BIOS_start();
    return (0);
}
```

Рисунок 2.6 – “Tasks” в BIOS

Слідує згадати, що дана плата являє собою RTOS і для неї існує аналог бібліотеки OpenSSL – WolfSSL, який містить в собі оптимізовану реалізацію алгоритмів хешування та шифрування при зборці бібліотеки для деякий вбудованих пристроїв. Ця бібліотека допомагає реалізовувати на платі функціонал TCP/UDP клієнтів або сервері та інше. Для захисту від SPA та DPA пропонується також використовувати особливості плати й виконувати в двох різних завдання функціонал алгоритму для одного й того ж повідомлення, але для різних ключів. Це дасть змогу скрити вірний ключ, адже операція виконується двічі. Також для попередження атакам за помилками в ще одному завданні можна запустити виконання алгоритму двічі.

2. *Пристрої без операційної системи.* Для аналізу особливостей багатопотоковості на пристроях, що не мають операційної системи, розглянемо мікроконтроллер TMS320F28027, чіп якої відноситься до покоління процесорів C2000, фірми Texas instruments. (Рисунок 2.7)

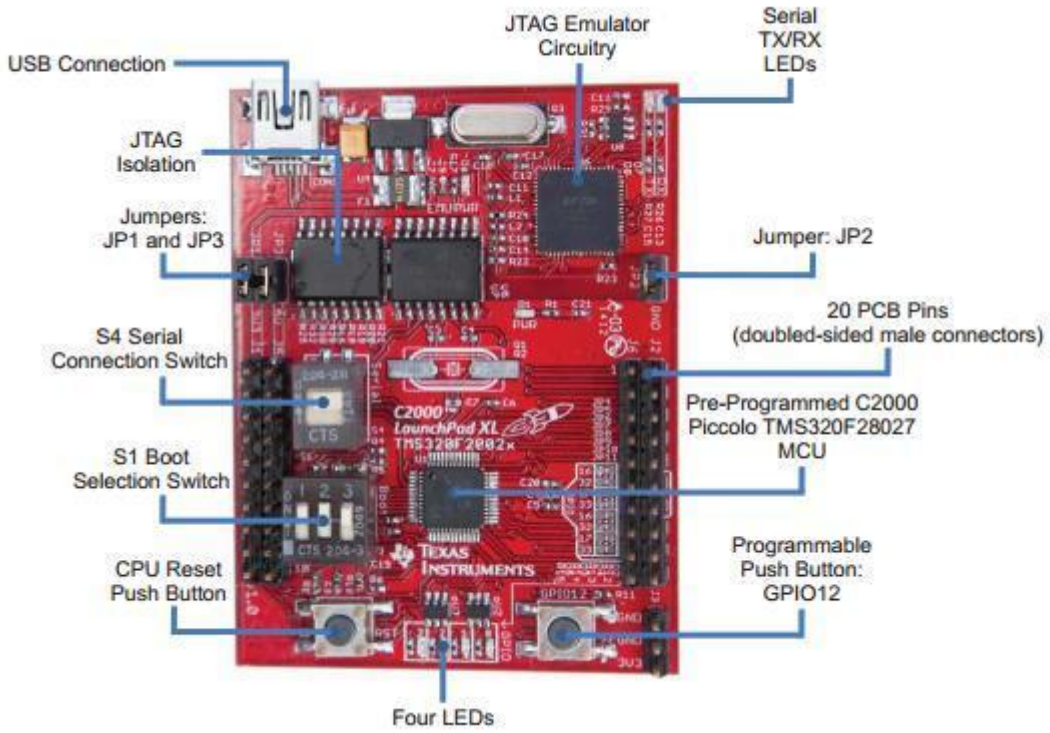


Рисунок 2.7 – Мікроконтролер TMS320F28027

Мікроконтролер не підтримує багатопотоковість і реалізація ідеї даної протидії може бути виконана лише програмно, при створенні реалізації алгоритму на пристрої. В цілому спосіб реалізації багатопотоковості на такого роду пристроях повністю залежить від фантазії програміста та його знань. Пропонується по таймеру, який виділяє максимально потрібний час для найскладнішого виду операцій, перемикати виконувані операції. При цьому потребуються достатньо великі зміни в дизайні алгоритму. Таким чином, можна гарантувати захист від атак за часом, так як кожна дія виконується однаковий період часу, а також проти атак за споживанням, адже на спектральній діаграмі спожитого сигналу буде не систематично зображені

виконувані операції. Це схоже на деякий вид рандомізації. При цьому слід враховувати, що виконання операції з великими числами на мікроконтролері дуже важко, адже, наприклад для TMS320F28027, розрядність складає 32 біти. Для оптимізації та дійсно практично потрібної реалізації криптосистеми в такому випадку, краще реалізовувати її на рідному асемблері мікроконтролера.

Висновок

В даному розділі було розглянуто роботу криптосистеми RSA. Зрозуміло, що одною з цілей аналізу стають операції піднесення у степінь та множення, через їх залежність від вхідних даних та явна помітність на діаграмі сигналу. Також часто використовувана китайська теорема про залишки для покращення швидкодії алгоритму, негативно впливає на сторонні канали видаючи багато інформації про виконувані операції, таким чином не рекомендується до використання алгоритму без прийнятних протидій до SCA.

Серед існуючих видів аналізу, Timing analysis та SPA є найбільш популярними та простими та в той же час результативними. Сама ідеї аналізувати криптосистеми по стороннім каналам походить від недосконалості системи та фізичних процесів, які лежать в сонові сучасної електроніки.

Варто зазначити, що існує дуже багато способів до протидії аналізу. Нажаль навіть половина з них не гарантує неможливість проведення успішних атак, а лише знижують ймовірність та підвищують час, що потребується на проведення більшої кількості замірів для різноманітних вхідних даних та умов. Зосереджуючись на згаданих вище най можливіших атаках (Timing analysis та SPA) можна виділити найбільш надійні методи:

- Рандомізація виконуваних операцій;
- Балансування спожитої енергії та часу;
- Апаратне приховання;

Звичайно слід враховувати, що вони мають результат тільки у поєднанні, а гарним доповненням для них може стати уникнення умовних переходів, якщо це можливо. Для попередження атак за помилками слід виконувати шифрування двічі, звісно це не гарантує повний захист від подібного виду атак, але значно підвищить надійність. Хоча слід враховувати збільшення часу на виконання шифрування, тому ця протидія повинна повністю виправдовувати себе. Де можливо використовувати багато потоковість, це краще роботи, таким чином може забезпечуватись гарна рандомізація та одночасне виконання операцій.

Усі перераховані протидії доцільно використовувати при великих потребах в конфіденційності, адже таке нагромадження додаткових операцій набагато збільшить складність та час виконання алгоритму. Насправді найкращим підходом біде повний ре-дизайн алгоритму з врахуванням потрібних видів захисту та його оптимізація під використовуваний вид обладнання, архітектуру та інше. Врахування особливостей апаратного функціоналу пристрою, можна на достатньо високому рівні реалізувати апаратне приховання. Таким чином, широко використовується управління годинниковими тактами та PWM. Звісно це потребує точних вимог та великого об’єму часу, але є доцільним для великих компаній з довготривалими проектами.

Також у розділі згадувався фізичний захист, й лише для того, щоб вказати на його існування, але він є зовсім недоцільним. Так само недоцільно використовувати додавання шуму, затримок та зменшувати амплітуду сигналу. Ці дії легко буде виявити при правильній цифровій обробці та отриманні частотного спектру сигналу. Вони насправді майже не впливають на аналіз.

Варта уваги ідея з осліпленням, яка через специфіку реалізації не зможе широко використовуватись.

3 ДОСЛІДЖЕННЯ РОБОТИ КРИПТОСИСТЕМИ ПО СТОРОННІМ КАНАЛАМ

Вступ

У даному розділі викладені результати досліджень роботи криптосистем за допомогою розробленого приладу. Також розглянуто будову прилад, спосіб збирання та передачі даних.

Наведені та проаналізовані сигнали споживання енергії криптосистеми RSA, що реалізована на двох мікроконтролерах TMS320F28027 та TM4F1294XL.

3.1 Принцип збирання даних

В основі збирання даних покладені наступні сподівання:

1. На досліджуваній схемі, що реалізує роботу криптосистеми, знаходиться доріжка, яка забезпечує постачання електроенергії для роботи мікроконтролера.
2. Далі ця дорожка перерізається у зручному місці та туди підключається резистор (Рисунок 3.1) великого номіналу для збільшення сили току.

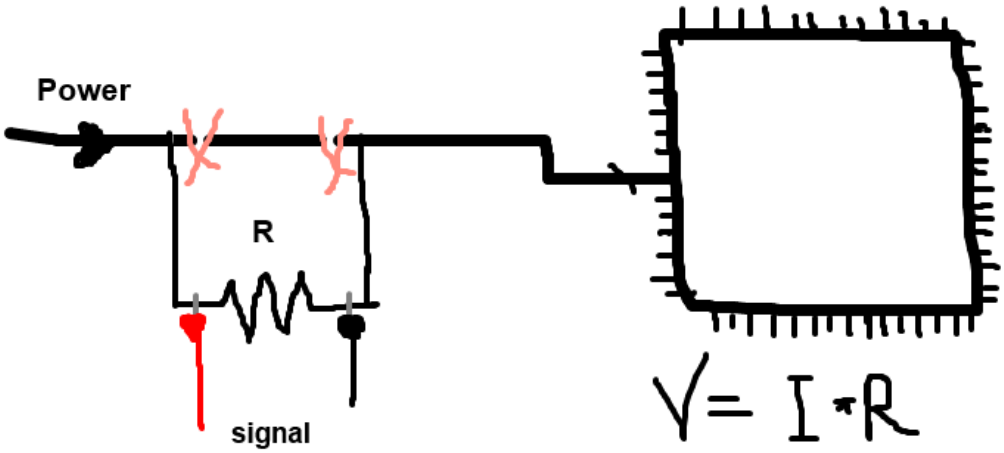


Рисунок 3.1 – Вимірювання сигналу

3. Різниця перепаду напруги на цьому резисторі і буде вимірюватись (Рисунок 3.1). Таким чином отримаємо показники споживаної енергії чіпом.

Так для TMS320F28027 аналізуючи схему плати можна побачити, що енергія з USB, що підключений до комп'ютера та живить плату, протікає через джампер JP1 (Рисунок 3.2).

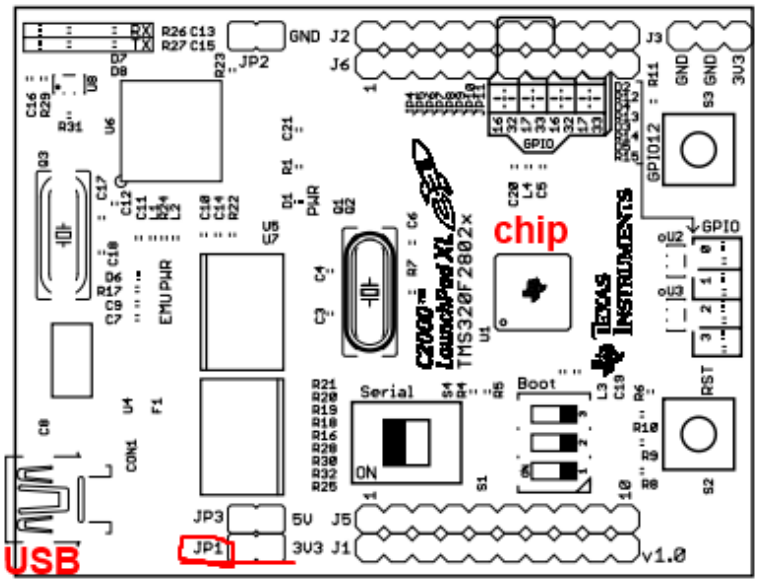


Рисунок 3.2 – Підключення до TMS320F28027

Далі там де на Рисунку 3.1 знімається сигнал слідує розроблена плата (Рисунок 3.3). Головне її завдання – це функціонувати, як підсилювач та дискретезатор сигналу. Це забезпечується підсилювальним каскадом на початку, потім сигнал йде на повторювач, а далі на ADC перетворювач.

Схема розроблена таким чином, щоб підтримувати напруги 3.3 V за допомогою відповідного стабілізатору. Сигнал подається на джампер J4. Сама плата не має програмується і всі виконувані нею функції забезпечуються апаратними засобами та підібраними елементами.

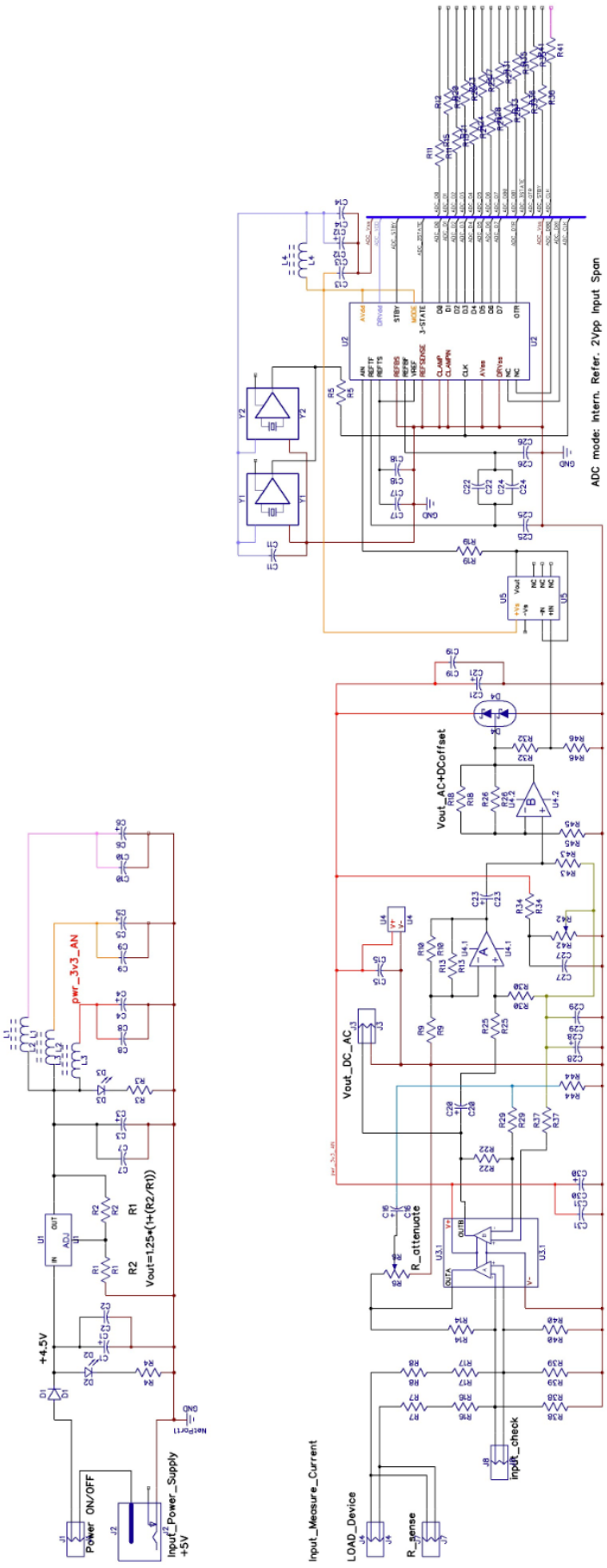


Рисунок 3.3 - Схема розробленої плати

Плата розроблена за допомогою пакету програм Dip Trace. Також там виконане її трасування, показане на Рисунку 3.5.

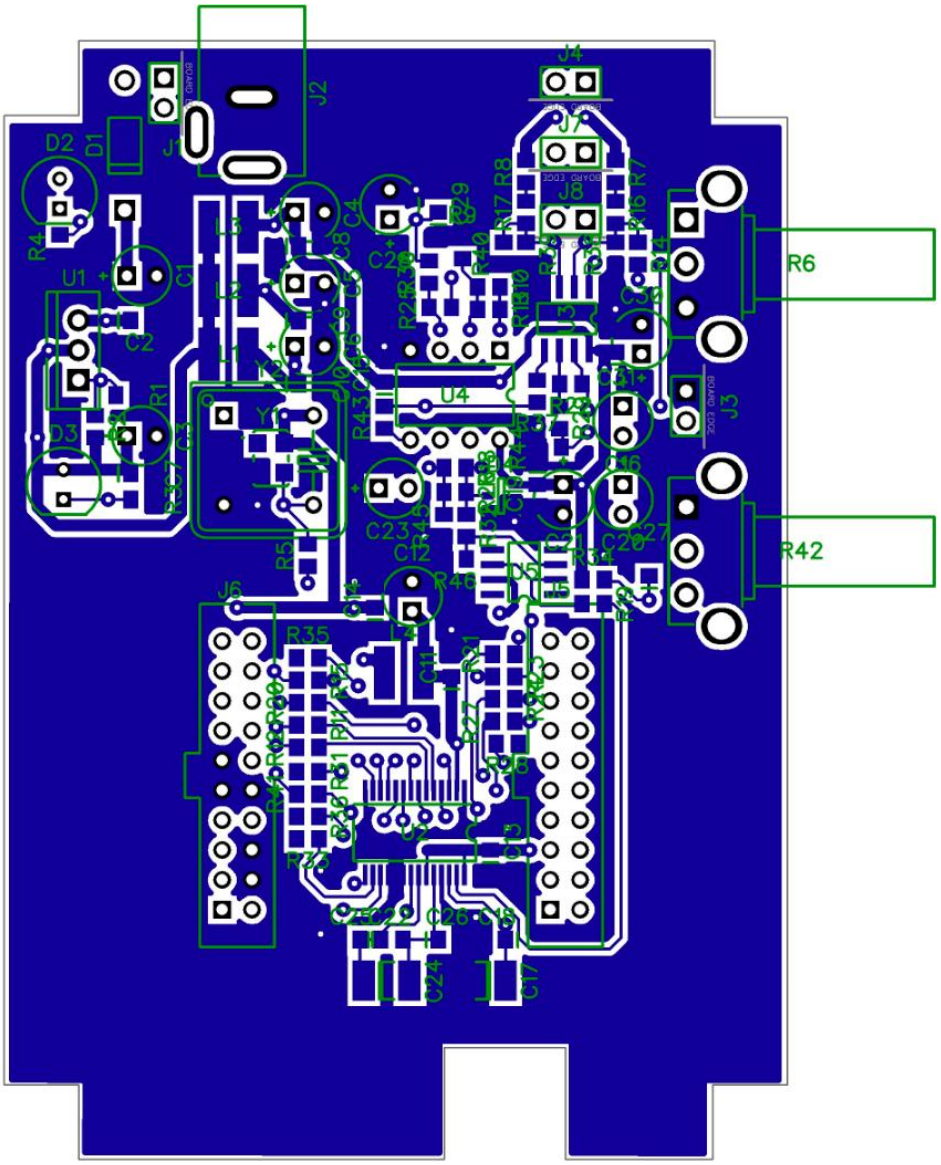


Рисунок 3.5 – Розводка схеми

Живиться вона від вставленої зверху перехідної плати, яка при цьому виконує й функцію спілкування з комп'ютером по USB. В якості даного комунікатора була вибрана CY7C68013A MINI BOARD компанії LCSOFT (Рисунок 3.4).

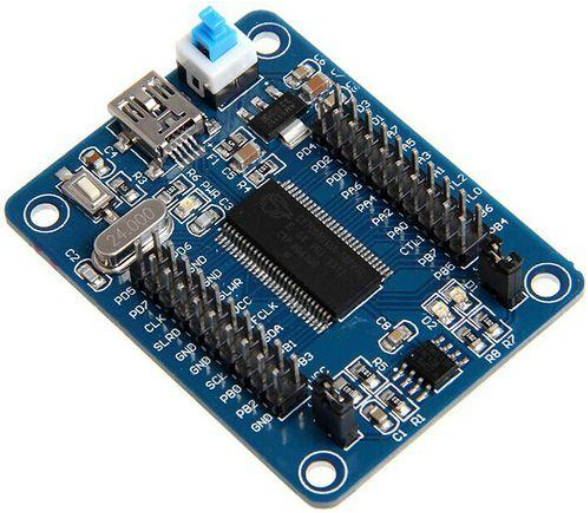


Рисунок 3.4 – USB конвертор

Сигнал, що передається з цільової плати проходить через таку схему та за домогою програматора на борту перехідної плати зберігається на комп’ютері у вигляді 8-бітного одно канального файлу, який дуже зручно відкривати програмами для обробки звуку.

Таким чином, маємо схему для збирання даних при роботі криптосистеми.

3.2 Специфіка обробки сигналу

Дана схема дискретизує вхідний сигнал, підсилює його та передає на комп’ютер для подальшого аналізу. При цьому присутні два підлаштовні резистора, що допомагають регулювати амплітуду та зсув сигналу.

Ідея їх роботи полягає в тому, щоб знайти робочу точку для сигналу. Вимірюваний сигнал має напругу 3.3 V, при цьому підключившись осцилографом до підлаштовних резисторів можна побачити як змінюється сила та розміщення сигналу по осі ординат.

Головна мета знайти максимальне підсилення амплітуди сигналу, щоб вона становила 3.3 V та положення умовного нуля для сигналу за допомогою підлаштування резистора зсуву.

Тільки після знаходження робочої точки, отримані заміри можна вважати актуальними для аналізу, та дроблення висновків щодо виконуваних операцій криптосистемою.

3.3 Заміри

При запущеній криптосистемі, що реалізує алгоритм RSA, очікується побачити таку поведінку споживання енергії, як показано на Рисунку 3.6.

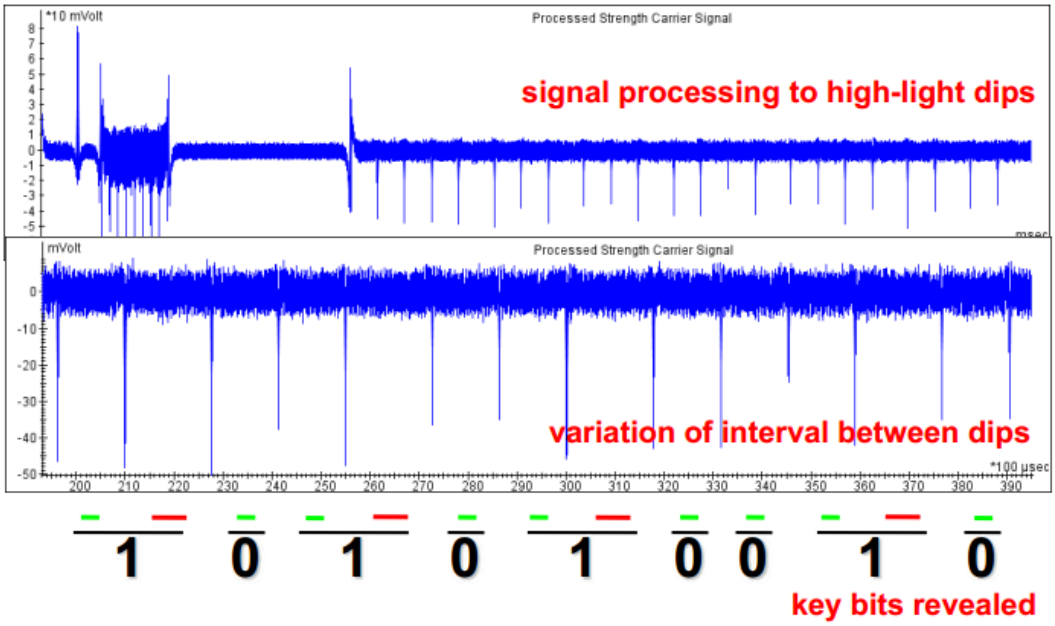


Рисунок 3.6 – RSA side-channel інформація

Звісно на реальних пристроях неможливо очікувати настільки просту поведінку та легкий аналіз криптосистеми. В дійсності сигнал буде більше нагадувати Рисунок 3.7.

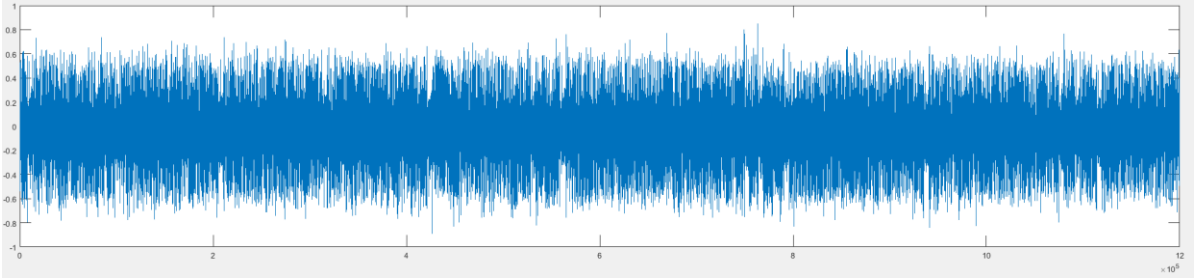


Рисунок 3.7 – Сигнал споживання реальної системи

Таким чином, не складно помітити, що кількість виконуваних операцій одночасно утворюють кіпу різночастотних гармонік, які разом складають інформацію про систему загалом. Насправді, така картина зовсім не означає, що процеси скриті і момент роботи криптографічного модулю не може бути визначений. Для прикладу розглянемо шифрування з протидіям у вигляді апаратного приховання та рандомізації. Для цього використаємо згадувану вище схему заміру даних (Рисунок 3.8).

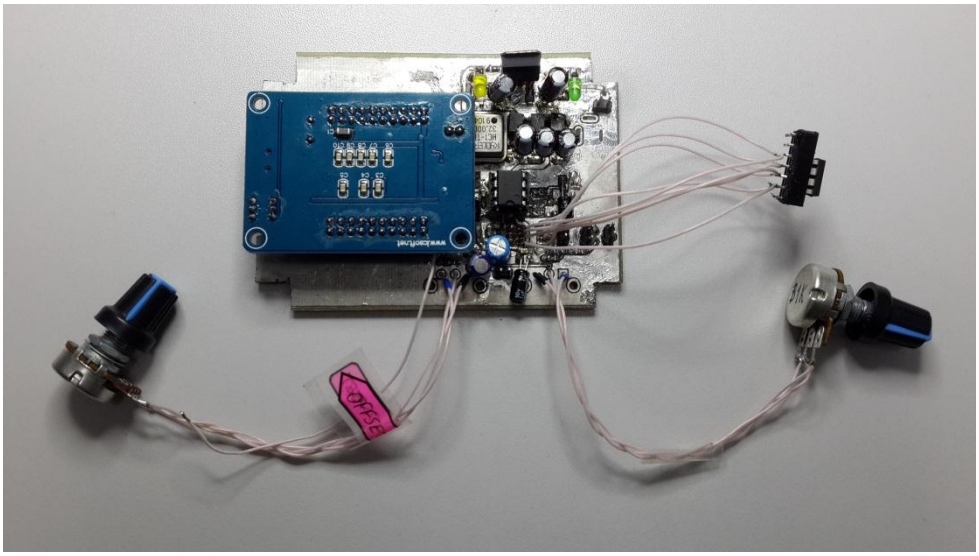


Рисунок 3.8 – Розроблена схема

Знімемо дані з розриву на JP1на платі TMS320F28027 (Рисунок 3.9).

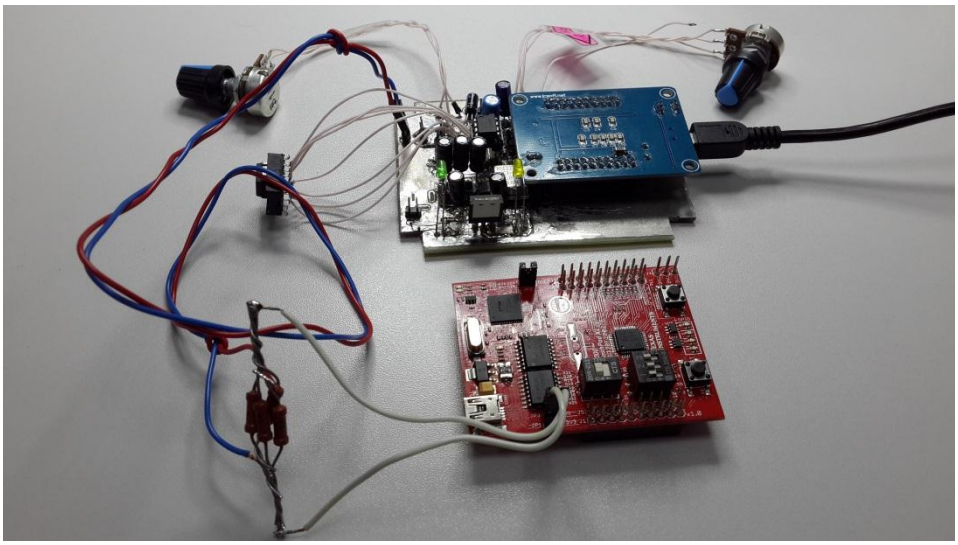


Рисунок 3.9 – Схема підключення

Подамо енергію на плати, та зробимо заміри. Результат отримуємо у вигляді однокального 8-бітного дискретизованого сигналу. Відкриваємо його за допомогою згаданої раніше програми обробки звуку Audacity (Рисунок 3.10).

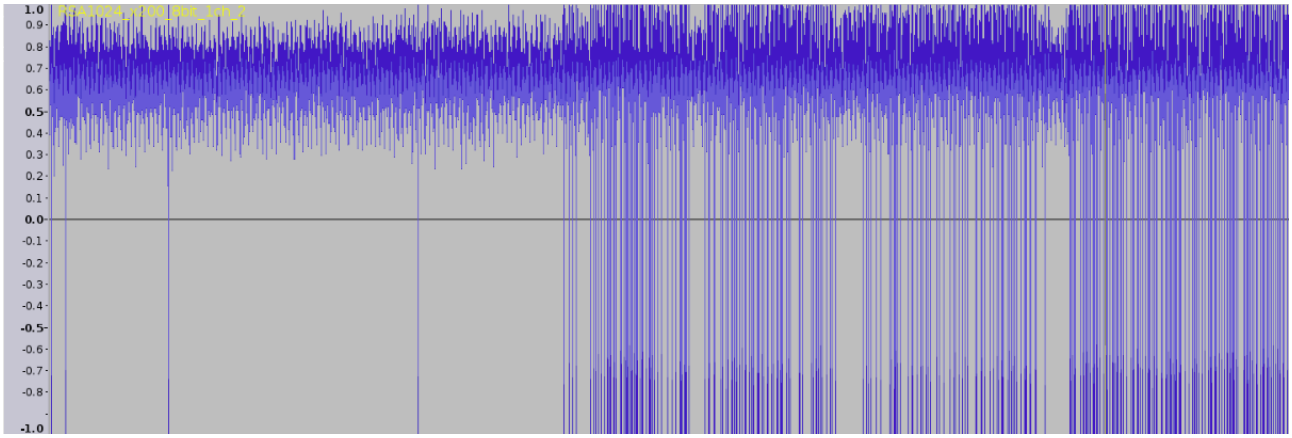


Рисунок 3.10 – Заміряний сигнал №1

З Рисунку 3.10 видно незрозумілі стрибки частот. Ця поведінка означає, що робоча точка, що регулюється підлаштовними резисторами була вибрана невірно. Поява таких піків, як результат, також включає в собі особливості програми Audacity. Для 8-бітного сигналу вона інтерпретує, як максимальне значення 254, а 255 викликає переповнення та різкий стрибок частоти. Програма трактує його як деяку дельта функцію. Для нормального аналізу потрібно нормалізувати сигнал стосовно використаного ADC, тобто вірно відрегулювати положення та амплітуду сигналу в рамках вікна аналого-цифрового перетворювача.

Відрегулювавши проводимо заміри знову та отримуємо сигнал, зображений на Рисунку 3.11. Сигнал заміряний під час роботи криптосистеми і хоча це не очевидно, шифрування циклічно відбувається під час активності роботи системи.

Головне завдання зараз – проаналізувати побачений сигнал, та знайти активність, що вибивається з загальної частоти, тобто виділити інформативні області з форми сигналу.

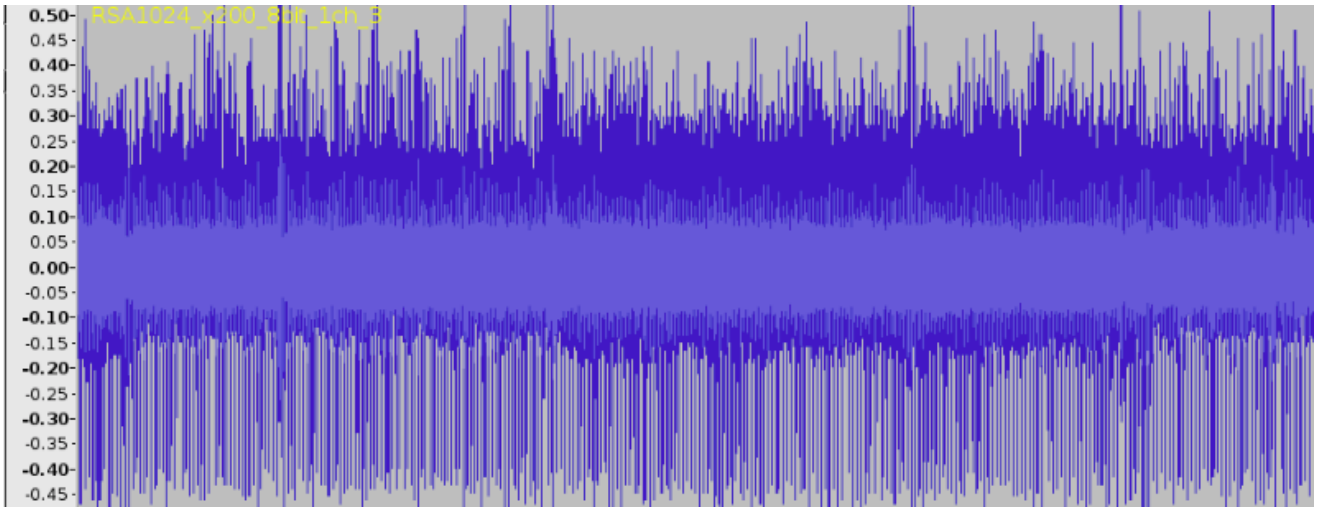


Рисунок 3.11 Заміряний сигнал №2

На Рисунку 3.12 виділена частина сигналу, яка одразу помітно, що вибивається з сигналу зміною своєї амплітуди.

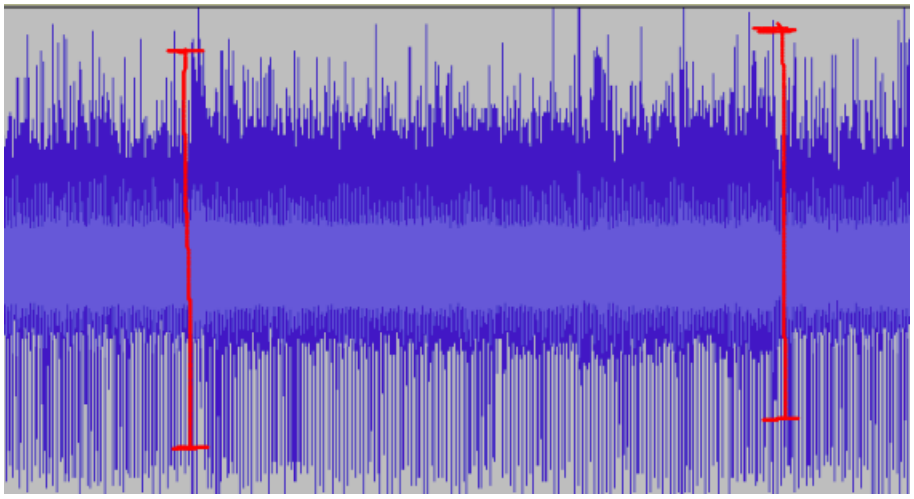


Рисунок 3.12 – Виділення інформативної області

Для подальшого аналізу користуємося методами цифрової обробки сигналів, а саме віконним перетворенням Фур'є з використанням вікна Хеммінга. Дані методи описані у першому розділі. Таким чином розкладаємо сигнал в спектр, за замовчанням, з довжиною вікна 256 (Рисунок 3.13).

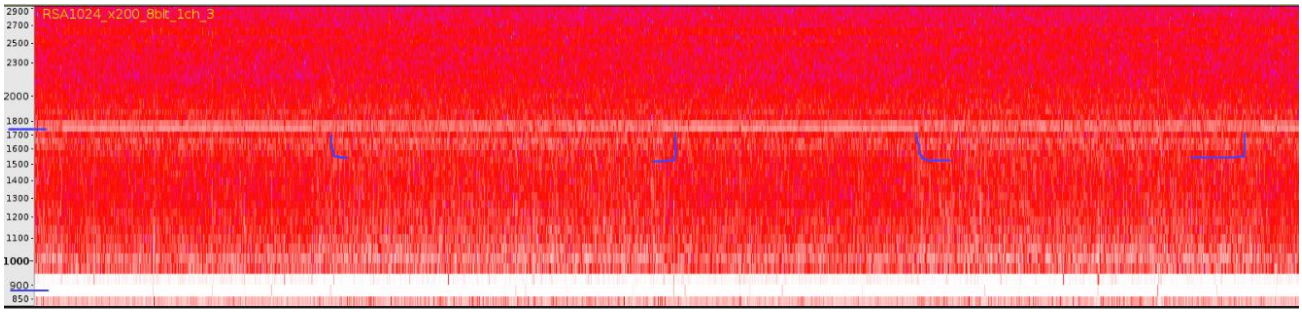


Рисунок 3.13 – Спектр сигналу №2 (W = 256)

Одразу помітні сильні частоти на приблизній позначці 900, та її друга гармоніка близько 1800. З деяким інтервалом помітна активність, що вибивається з сталої частоти, це означає, що відбуваються якісь процеси при роботі системи. Тим не менш, ширина вікна досить мала, щоб судити про вірне визначення частоти. При меншій ширині вікна ми лише можемо точно локалізувати у часі виконання процесів. Тому збільшимо ширину вікна для спектрального аналізу (Рисунок 3.14).

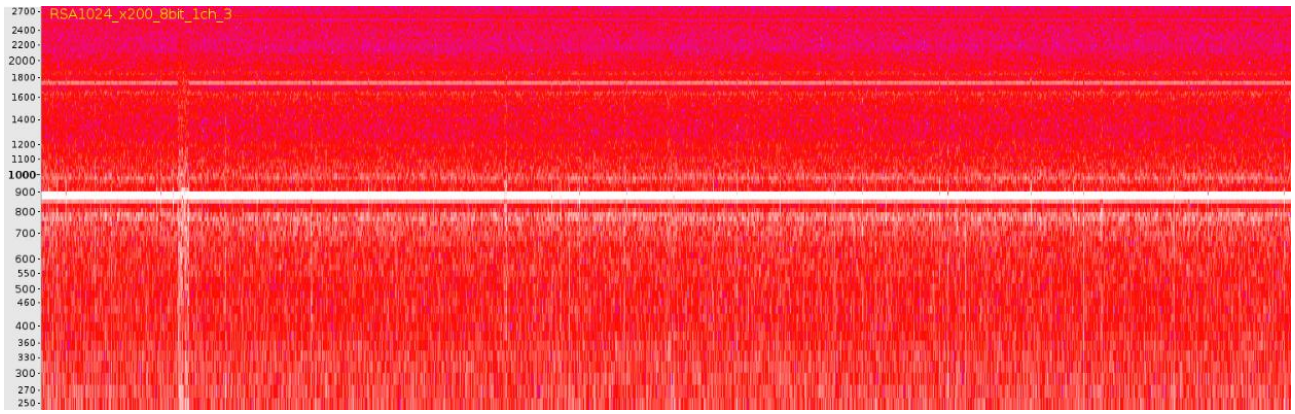


Рисунок 3.14 - Спектр сигналу №2 (W = 8192)

На Рисунку 3.14 видно, що процеси в яких ми зацікавлені зникли, через парадокс неможливості визначення точної частоти та її локалізації у часі. Тим не менш, отримавши точне значення частоти та її гармонік, сигнал фільтрується, а після цього вже досліджується в часі. Слід зазначити, що для фільтрації можна використовувати, як можливості самої програми, так і власні розробки, та враховувати при фільтруванні охоплювати більшу частину близьких частот

для менших втрат інформативності. Крім того, найбільшу цінність при фільтруванні складає не основна гармоніка, а більш високочастотні, адже вони несуть набагато більшої інформації про точний стан системи у часі, а головна більше схожа на огинаючу синусоїду.

Відфільтруємо сигнал за тими частотами і насправді побачимо, що активність, яка була помітна й без спектру й була частиною цільових частот (Рисунок 3.15).

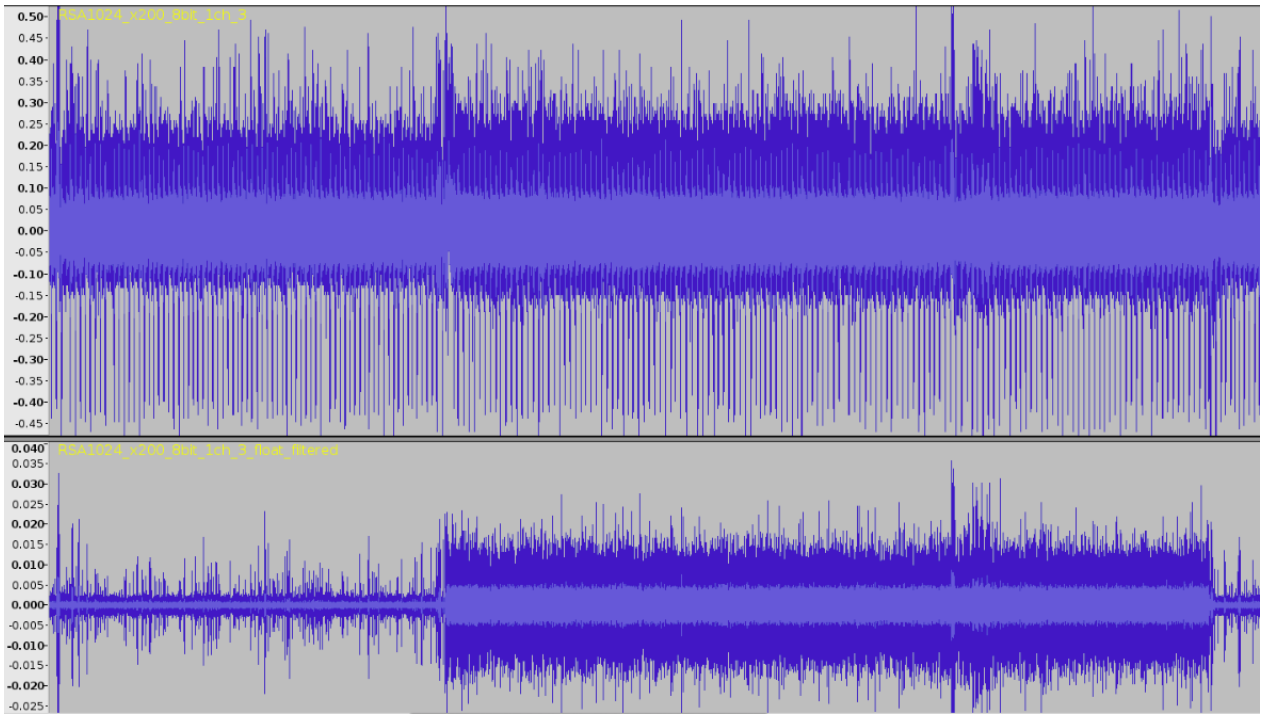


Рисунок 3.15 – Фільтрація сигналу №2

Проаналізуємо спектр відфільтрованого сигналу (Рисунок 3.16 (a, b, c)). Видно, що виділились гармоніки саме згадуваних вище частот.

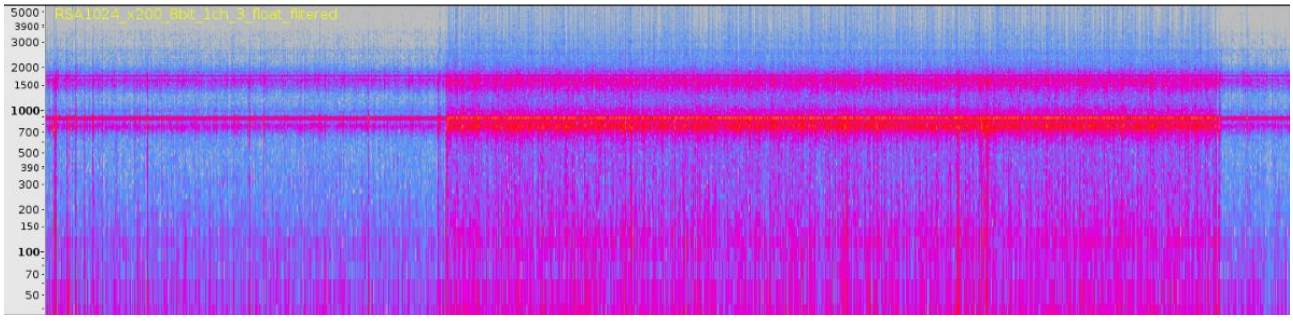


Рисунок 3.16 (a) – Спектр відфільтрованого сигналу №2 (W = 16384)

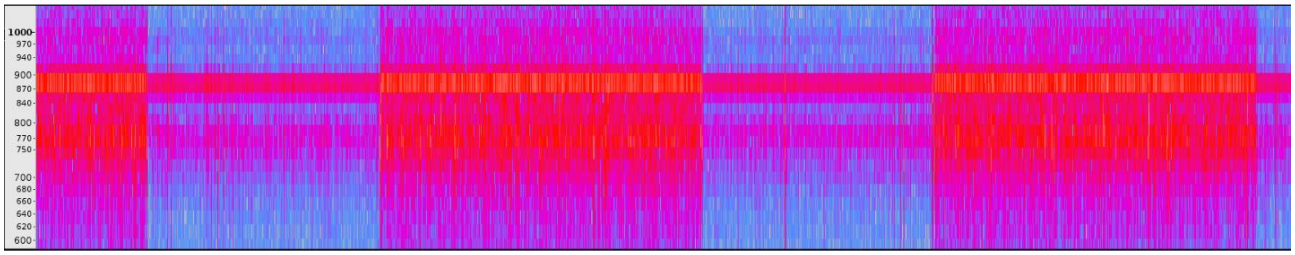


Рисунок 3.16 (b) – Спектр відфільтрованого сигналу №2 (W = 16384)

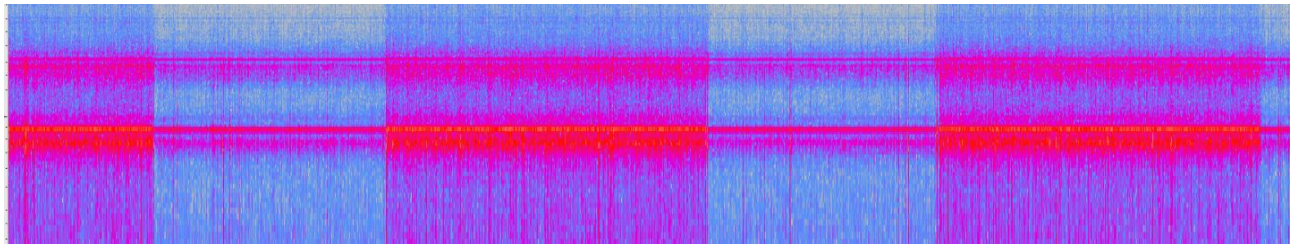


Рисунок 3.16 (c) – Спектр відфільтрованого сигналу №2 (W = 16384)

Отриманий вище спектр, досліджують методами кореляційного аналізу, що можуть з накладання патернів, які простежуються на Рисунок 3.16 (c) виділити схожу поведінки та обчислити 4 ключі, один з яких використовувався в шифруванні. Висновку щодо досліджуваного сигналу можна прийти й аналізуючи Рисунок 3.16 (b). На ньому під гармонікою чітко простежуються інформаційні сигнали, що споживають енергію.

Ще один замір додав інформації (Рисунок 3.17). Добре помітно меандро-подібний характер на спектрограмі, що свідчить про періодичність деякого процесу. Спектрограма зроблена для великого вікна, що розмиває паразитивні частоти біля основної та знижує його інформативність, тим не менш можна виділити область подальшого аналізу.

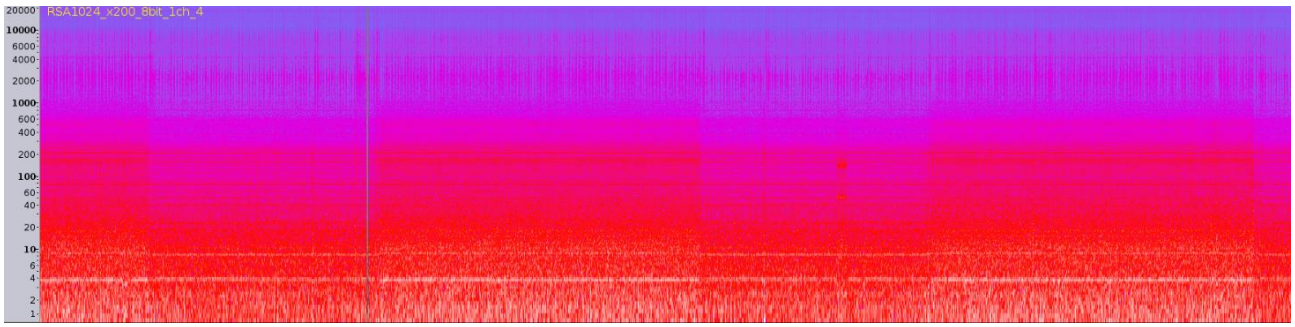


Рисунок 3.17 – Спектр сигналу №3 (W = 16384)

При локалізації у часі бачимо набагато чіткішу картину зміни сигналу на спектрі (Рисунок 3.18).

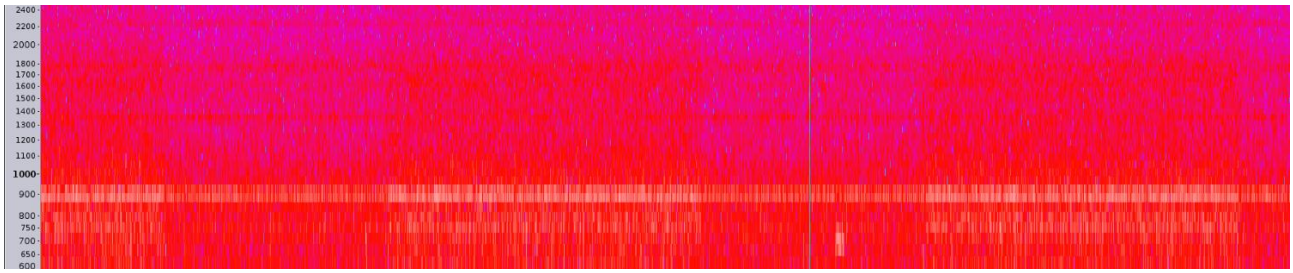


Рисунок 3.18 - Спектр сигналу №3 (W = 4096)

Висновок

У даному розділі було представлено проведення аналізу вибраних у розділі 2 протидій, а саме апаратне приховання та рандомізація. Картина спектру сигналу споживання за даних умов на прийнятному рівні забезпечую надійність крипто модулю, та незважаючи на можливість виділити активність, її локалізація у часі настільки складна, що не приносить бажаних результатів за досліджуваний проміжок часу.

Слід зазначити, що незважаючи на вдачу з даними протидіями, такі заходи не можуть гарантувати однозначної безпеки для будь-якої апаратної реалізації RSA. Для кожного випадку повинна бути проаналізована система, та оточення які впливають на споживання та створюють загальну картину роботи системи. Це обумовлюється специфікою використовуваного обладнання.

Для забезпечення надійності криптосистеми слід писати код, точно уявляючи як це може вплинути на роботу системи та виділивши інформаційні гармоніки додавати туди рандомізацію та преривання. Більш універсальний спосіб – зміна частоти роботи процесора в непередбачувані моменти часу, таким чином, в кращому випадку, не можна виділити частоту на які відбувається інформативний процес. Це може бути обійдено нормалізуванням частоти, але таке займає дуже велику кількість часу і не дає гарантій на досягнення результату.

4 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

Вступ

Стартап як форма малого ризикового (венчурного) підприємництва впродовж останнього десятиліття набула широкого розповсюдження у світі через зниження бар'єрів входу в ринок (із появою Інтернету як інструменту комунікацій та збуту стало простіше знаходити споживачів та інвесторів, займатись пошуком ресурсів, перетинати кордони між ринками різних країн), і вважається однією із наріжних складових інноваційної економіки, оскільки за рахунок мобільності, гнучкості та великої кількості стартап-проектів загальна маса інноваційних ідей зростає.

Проте створення та ринкове впровадження стартап-проектів відзначається підвищеною мірою ризику, ринково успішними стає лише невелика частка, що за різними оцінками складає від 10% до 20%. Ідея стартап-проекту, взята окремо, не вартує майже нічого: головним завданням керівника проекту на початковому етапі його існування є перетворення ідеї проекту у працюючу бізнес-модель, що починається із формування концепції товару (послуги) для визначеної клієнтської групи за наявних ринкових умов.

Розроблення та виведення стартап-проекту на ринок передбачає здійснення низки кроків, в межах яких визначають ринкові перспективи проекту, графік та принципи організації виробництва, фінансовий аналіз та аналіз ризиків і заходи з просування пропозиції для інвесторів. Узагальнено етапи розроблення стартап-проекту можна подати таким чином:

1. Маркетинговий аналіз стартап-проекту

В межах цього етапу:

- розробляється опис самої ідеї проекту та визначаються загальні напрями використання потенційного товару чи послуги, а також їх відмінність від конкурентів;
- аналізуються ринкові можливості щодо його реалізації;
- на базі аналізу ринкового середовища розробляється стратегія

ринкового впровадження потенційного товару в межах проекту.

2. Організація стартап-проекту

В межах цього етапу:

- складається календарний план-графік реалізації стартап-проекту;
- розраховується потреба в основних засобах та нематеріальних активах;
- визначається плановий обсяг виробництва потенційного товару, на основі чого формулюється потреба у матеріальних ресурсах та персоналі;
- розраховуються загальні початкові витрати на запуск проекту та планові загальногосподарські витрати, необхідні для реалізації проекту.

3. Фінансово-економічний аналіз та оцінка ризиків проекту

В межах цього етапу:

- визначається обсяг інвестиційних витрат;
- розраховуються основні фінансово-економічні показники проекту (обсяг виробництва продукції, собівартість виробництва, ціна реалізації, податкове навантаження та чистий прибуток) та визначаються показники інвестиційної привабливості проекту (запас фінансової міцності, рентабельність продажів та інвестицій, період окупності проекту);
- визначається рівень ризикованості проекту, визначаються основні ризики проекту та шляхи їх запобігання (реагування на ризики).

4. Заходи з комерціалізації проекту

Цей етап спрямовано на пошук інвесторів та просування інвести-ційної пропозиції (оферти). Він передбачає:

- визначення цільової групи інвесторів та опису їх ділових інтересів;
- складання інвест-пропозиції (оферти): стислої характеристики проекту для попереднього ознайомлення інвестора із проектом;
- планування заходів з просування оферти: визначення

комунікаційних каналів та площадок та планування системи заходів з просування в межах обраних каналів;

- планування ресурсів для реалізації заходів з просування оферти.\

Означені етапи, реалізовані послідовно та вчасно – створюють передумови для успішного ринкового старту. Проте фахівці зі створення та розвитку стартап-проектів окремо відзначають, що відсутність маркетингових знань та умінь, що уможливлюють розробку ринково затребуваного проекту із вихідної ідеї, є основною причиною високого рівня банкрутств стартап-компаній, і ця проблема може бути вирішена за рахунок навчання винахідників. Відповідно, основним призначенням даних Методичних рекомендацій є надання студентам знань щодо суті, основних принципів розроблення стратегії ринкового впровадження та маркетингового управління інноваційними стартап-проектами у промислових галузях економіки, використання ефективних маркетингових інструментів просування високотехнологічних продуктів виробництва та послуг.

4.1 Опис ідеї проекту

В межах підпункту було проаналізовано і подано у вигляді таблиць:

- зміст ідеї (що пропонується);
- можливі напрямки застосування;
- основні вигоди, що може отримати користувач товару (за кожним напрямком застосування);
- чим відрізняється від існуючих аналогів та замінників;

Перші три пункти подані у вигляді таблиці (таблиця 4.1) і дають цілісне уявлення про зміст ідеї та можливі базові потенційні ринки, в межах яких потрібно шукати групи потенційних клієнтів.

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
Реалізація алгоритму RSA, яка включає наступні протидії аналізу: рандомізація, апаратне приховання, шифрування двічі та многопоточність.	1. Wifi модулі	1. Забезпечення цілісності та конфіденційності даних
	2.Вбудовані пристрої для шифрування трафіку	2. Забезпечення високого рівня надійності, що ставиться перед цільовим вбудованим приладом

Аналіз потенційних техніко-економічних переваг ідеї (чим відрізняється від існуючих аналогів та замінників) порівняно із пропозиціями конкурентів передбачає:

- визначення переліку техніко-економічних властивостей та характеристик ідеї (орієнтований можливий перелік властивостей та характеристик подано у додатку А);
- визначення попереднього кола конкурентів (проектів-конкурентів) або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проведення збір інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів-конкурентів відповідно до визначеного вище переліку;
- проведення порівняльного аналізу показників: для власної ідеї визначені показники, що мають а) гірші значення (W, слабкі); б) аналогічні (N, нейтральні) значення; в) кращі значення (S, сильні) (таблиця 4.2).

Визначений перелік слабких, сильних та нейтральних характеристик та властивостей ідеї потенційного товару є підґрунтям для формування його конкурентоспроможності.

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№	*Техніко-економічні характеристики ідеї*	*(потенційні) товари/концепції конкурентів*		*W (слабка сторона)*	*N (нейтральна сторона)*	*S (сильна сторона)*
		Мій проект	*Контроллер*			
1	Безпека	Ефективна протидія аналізу по стороннім каналам	Можливі деякі протидії (додавання шуму)			+
2	Собівартість	Середня	Висока			+
3	Універсальність	Підходить не для всіх пристроїв	Підтримує багато архітектур	+		
4	Швидкодія шифрування	Низька	Висока	+		

4.2 Технологічний аудит ідеї проекту

В межах даного підрозділу було проведено аудит технології, за допомогою якої можна реалізувати ідею проекту (технології створення товару).

Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (таблиця 4.3):

- за якою технологією буде виготовлено товар згідно ідеї проекту?
- чи існують такі технології, чи їх потрібно розробити/доробити?
- чи доступні такі технології авторам проекту?

За результатами аналізу таблиці 4.3 зроблено висновок, про можливість реалізації проекту. Технологічним шляхом реалізації проекту було обрано такі технології, як TM4F1294NCDT, CCS 7 та WolfSSL через їх доступність, технологічність та невелику вартість.

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологій*
1	Мікроконтролер	TMS320F28027	У наявності	Доступно.
2	Мікроконтролер	TM4F1294NCDT	У наявності	Доступно.
3	Середа розробки	CCS 7	У наявності	Доступно на усіх ОС.
4	Шифрування	WolfSSL	У наявності	Доступно на TM4F1294NCDT.
5	Шифрування	Embedded реалізація	Немає у наявності	Доступно на усіх мікроконтролерах.
Обрана технологія реалізації ідеї проекту: TM4F1294NCDT + CCS 7 + WolfSSL				

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Спочатку було проведено аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (таблиця 4.4).

Середню норму рентабельності в галузі було порівняно із банківським відсотком на вкладення. Останній є меншим, тому є сенс вкладати гроші саме у цей проект.

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1	Кількість головних гравців, од	3
2	Загальний обсяг продаж, грн/ум.од	1 700 000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Грошові запаси
5	Специфічні вимоги до стандартизації та сертифікації	Немає
6	Середня норма рентабельності в галузі , %	R = 28%

За результатами аналізу таблиці 4.4 було зроблено висновок, що ринок є відносно привабливим для входження.

Надалі були визначені потенційні групи клієнтів, їх характеристики, та сформовано орієнтовний перелік вимог до товару для кожної групи (таблиця 4. 5).

Після визначення потенційних груп клієнтів було проведено аналіз ринкового середовища: складено таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (таблицяі 4.6, 4.7).

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
	Потреба у надійному алгоритмі шифрування конфіденційних даних.	Компанії, що розробляють вбудовані пристрою з можливістю шифрування секретних даних.	В залежності від способу використання алгоритму: для шифрування чи цифрових підписів.	Швидкодія, надійність та безпечність.

Після визначення потенційних груп клієнтів було проведено аналіз ринкового середовища: складено таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (таблицяі 4.6, 4.7).

Ринкові можливості - це сприятливі обставини, які підприємство може використовувати для отримання переваг. Як приклад ринкових можливостей можна привести погіршення позицій конкурентів, різке зростання по-питу, появу нових технологій виробництва продукції, зростання рівня доходів населення і т. п. Слід зазначити, що можливостями з погляду SWOT-аналізу є не всі можливості, які існують на ринку, а тільки ті, які можна використовувати

Ринкові загрози - події, настання яких може несприятливо вплинути на підприємство. Приклади ринкових загроз: вихід на ринок нових конкурентів, зростання податків, зміна смаків покупців, зниження народжуваності й т. п.

- чинники попиту (тут доцільно взяти до уваги місткість ринку, темпи його зростання або скорочення, структуру попиту на продукцію підприємства і т. ін.);
- чинники конкуренції (слід врахувати кількість основних конкурентів,

наявність на ринку товарів-замінників, висоту бар'єрів входу на ринок і виходу з нього, розподіл ринкових часток між основними учасниками ринку і т.ін.);

- чинники збуту (необхідно надати увагу кількості посередників, наявності сіток розподілу, умовам поставок матеріалів та комплектуючих і т. ін.);
- економічні чинники (враховується курс гривні (долара, євро), рівень інфляції, зміна рівня доходів населення, податкова політика держави і т.ін.);
- політичні і правові чинники (оцінюється рівень політичної стабільності в країні, рівень правової письменності населення, рівень законослухняності, рівень корумпованості влади і т.ін.);
- науково-технічні чинники (звичайно береться до уваги рівень розвитку науки, ступінь упровадження інновацій (нових товарів, технологій) в промислове виробництво, рівень державної підтримки розвитку науки і т. ін.);
- соціально-демографічні чинники (слід врахувати чисельність і статеву та вікову структури населення регіону, в якому працює підприємство, рівень народжуваності і смертності, рівень зайнятості населення і т.ін.);
- соціально-культурні чинники (звичайно враховуються традиції і система цінностей суспільства, існуюча культура споживання товарів і послуг, наявні стереотипи поведінки людей і т. ін.);
- природні і екологічні чинники (враховується кліматична зона, в якій працює підприємство, стан навколишнього середовища, відношення громадськості до захисту навколишнього середовища і т.ін.);
- міжнародні чинники (серед них враховується рівень стабільності в світі, наявність локальних конфліктів і т. ін.).

Таблиця 4.6 – Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
	Конкуренція	Поява уніфікованого, дешевого та зручного пристрою з реалізацією RSA без side-channel інформації.	1. Передбачити додаткові переваги власного проекту для того, щоб повідомити про них саме після виходу міжнародної компанії на ринок. 2. Обрати нову цільову аудиторію і зосередитися на ній
	Економічний	Подорожчання мікроконтролерів.	Оптимізація програмного продукту, для можливості його запуску на більш бюджетних пристроях.
	Науковий	Розроблення нових способів аналіз інформації по стороннім каналам.	Відстежування публікацій на дану тематику, відвідування RSA конференції, та проведеннях власних досліджень, для передбачення виникнення даної загрози.

Таблиця 4.7 – Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
	Науково-технічний	Тенденція до випуску мікроконтролерів з криптосистемою, яка не несе інформації по стороннім каналам.	Розробка нових методів протидії на основні проаналізованої добутої інформації при роботі криптосистеми по її стороннім атакам.
	Попит	Більш широкі вимоги до безпеки у всіх сферах життя.	Постійна підтримка продукту.

Надалі було проведено аналіз пропозиції: визначили загальні риси конкуренції на ринку (таблиця 4.8).

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства*
Вказати тип конкуренції: монополістична конкуренція.	Існує декілька фірм-конкурентів.	Підтримка якості продукту та постійні нововведення.
За рівнем конкурентної боротьби: Міжнародний.	Фірми-конкуренти знаходяться в інших країнах.	Адаптація продукту як для вітчизняних так і для зарубіжних клієнтів.
За галузевою ознакою: внутрішньогалузева.	Продукт використовується лише всередині даної галузі.	Постійне вдосконалення продукту.
Конкуренція за видами товарів: товарно-видова.	Види товарів однакові.	Створити продукт, що враховує сильні і слабкі сторони конкурентів.
За характером конкурентних переваг: нецінова.	Вдосконалення протидій.	Зниження ціни на продукт та підтримка його якості.
За інтенсивністю: марочна.	Бренди існують і конкурують.	PR, реклама, просування бренду.

Було проведено аналіз конкуренції у галузі за моделлю М. Портера (таблиця 4.9). М. Портер вирізняє п’ять основних факторів (Рисунок 4.1), що впливають на привабливість вибору ринку з огляду на характер конкуренції.

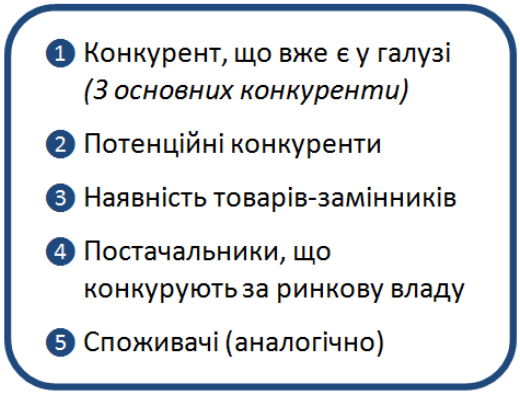


Рисунок 4.1 – Модель Портера

Сильні позиції компанії за кожним з факторів означають її можливості забезпечити необхідні темпи обороту капіталу та її здатність впливати на інших агентів ринку, диктуючі їм власні умови співпраці. Характеристики факторів моделі відрізняються для різних галузей та змінюються із часом. Сила кожного фактору є функцією від структури галузі та її техніко-економічних характеристик.

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	*Потенційні конкуренти*	*Постачальники*	*Клієнти*	*Товари-замінники*
Складові аналізу	NXP, VLSI	Наявність вже існуючих рішень	-	Контроль якості продукту	Поява уніфікованого та більш швидкого методу шифрування
Висновки:	Доволі інтенсивна конкурентна боротьба з вже закріпившимися на ринку гравцями.	Є можливості виходу на ринок, але є і конкуренти. Строки – 8 місяців.	-	Клієнти диктують усі умови роботи на ринку.	Перехід до абсолютного нового алгоритму шифрування, що гарантує більшу надійність за швидкодію.

За результатами аналізу таблиці 4.9 було зроблено висновок про можливість роботи на ринку з огляду на конкурентну ситуацію. Також було зроблено висновок щодо характеристик, які повинен мати проект, щоб бути конкурентноспроможним на ринку. Цей висновок був врахований при формулюванні переліку факторів конкурентноспроможності у наступному пункті.

На основі аналізу конкуренції, проведеного в таблиці 4.9, а також із урахуванням характеристик ідеї проекту (таблиця 4.2), вимог споживачів до

товару (таблиця 4.5) та факторів маркетингового середовища (таблиці 4.6, 4.7) визначається та обґрунтовується перелік факторів конкурентоспроможності. Аналіз оформлюється за таблицею 4.10

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)*
	Протидія методам аналізу по стороннім каналам	Надійність та висока безпека, гарантована розробленим рішенням.
	Ціна	Дане рішення не потребує дорогого додаткового обладнання та матеріалів, а достатньо лише програмного рішення та готового чіпу.

За визначеними факторами конкурентоспроможності (таблиця 4.10) проведено аналіз сильних та слабких сторін стартап-проекту (таблиця 4.11).

Таблиця 4.11 – Порівняльний аналіз сильних та слабких сторін

№ п/п	*Фактор конкурентоспроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні*						
			–3	*–2*	*–1*	*0*	*+1*	*+2*	*+3*
1	Протидія методам аналізу по стороннім каналам	17		+					
2	Ціна	18	+						

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) (таблиця 4.12) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (таблиця 4.11).

Перелік ринкових загроз та ринкових можливостей було складено на основі аналізу факторів загроз та факторів можливостей маркетингового середовища. Ринкові загрози та ринкові можливості є наслідками (прогнозованими результатами) впливу факторів, і, на відміну від них, ще не є

реалізованими на ринку та мають певну ймовірність здійснення. Наприклад: зниження доходів потенційних споживачів – фактор загрози, на основі якого можна зробити прогноз щодо посилення значущості цінового фактору при виборі товару та відповідно, – цінової конкуренції (а це вже – ринкова загроза).

Таблиця 4.12 – SWOT- аналіз стартап-проекту

Сильні сторони: ціна, надійність	Слабкі сторони: не універсальність, низька швидкість шифрування
Можливості: більш широке розповсюдження технологій з підтримкою протидій, поява нових технологій протидії SCA.	Загрози: усунення з ринку конкурентами, зміна потреб користувачів

На основі SWOT-аналізу було розроблено альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок (див. таблицю 5.9, аналіз потенційних конкурентів). Визначені альтернативи були проаналізовані з точки зору строків та ймовірності отримання ресурсів (таблиця 4.13).

Таблиця 4.13 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтовний комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
1	Розробка програмного продукту, PR, просування бренду	80%	10 місяців
2	Розробка програмного продукту, безкоштовне розповсюдження	70%	7 місяців

Після аналізу було обрано альтернативу №2.

4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: було проведено опис цільових груп потенційних споживачів (таблиця 4.14).

Таблиця 4.14 – Вибір цільових груп потенційних споживачів

№ п/п	*Опис профілю цільової групи потенційних клієнтів*	*Готовність споживачів сприйняти продукт*	*Орієнтовний попит в межах цільової групи (сегменту)*	*Інтенсивність конкуренції в сегменті*	*Простота входу у сегмент*
1	Компанії, що впроваджують конфіденційність даних	Невисока	Середній	Висока	Низька
2	Всі компанії, що володіють особистими даними клієнтів	Невисока	Високий	Невисока	Середня
Які цільові групи обрано: 2					

За результатами аналізу потенційних груп споживачів було обрано цільову групу, для якої буде запропоновано даний товар, та визначено стратегію охоплення ринку - стратегію концентрованого маркетингу(компанія зосереджується на одному сегменті).

Для роботи в обраних сегментах ринку сформовано базову стратегію розвитку (таблиця 4.15).

За М. Портером, існують три базові стратегії розвитку, що відрізняються за ступенем охоплення цільового ринку та типом конкурентної переваги, що має бути реалізована на ринку (за витратами або визначними якостями товару).

Стратегія лідерства по витратах передбачає, що компанія за рахунок чинників внутрішнього і/або зовнішнього середовища може забезпечити більшу, ніж у конкурентів маржу між собівартістю товару і середньо-ринковою ціною (або ж ціною головного конкурента). Зокрема, ця стратегія припускає, що за рахунок великих можливостей по об'ємах збуту товарів (портфеля укладених контрактів на постачання) і продуктивності підприємство може добитися менших витрат. Ця стратегія зазвичай тісно пов'язана з можливістю досягнення ефекту масштабу і досвіду.

Компанії, що вибирають цю стратегію, проводять ретельний контроль за постійними витратами, знижують виробничі, збутові і рекламні витрати, проводять інвестиції, спрямовані на зменшення витрат, ретельне опрацювання конструкції нових товарів.

Переваги стратегії за Ж.-Ж. Ламбеном:

- фірма здатна протистояти своїм прямим конкурентам навіть у разі цінової війни і в змозі отримувати прибуток при ціні, мінімально допустимій для конкурентів;
- сильні клієнти не можуть добитися зниження ціни нижче рівня, прийнятного для найбільш сильного конкурента;
- низькі витрати забезпечують захист проти сильних постачальників, оскільки дають фірмі велику гнучкість у разі підвищення вхідних витрат;
- низькі витрати створюють бар'єр входу для нових конкурентів і одночасно хороший захист проти товарів-замінників.

В ході конкурентної боротьби з використанням цієї стратегії з ринку вимушені будуть піти фірми, менш ефективні з точки зору величини і структури витрат, нездібні до проведення технологічних новацій, спрямованих на зниження витрат.

Стратегія диференціації передбачає надання товару важливих з точки зору споживача відмітних властивостей, які роблять товар відмінним від товарів

конкурентів. Така відмінність може базуватися на об’єктивних або суб’єктивних, відчутних і невідчутних властивостях товару(у ширшому розумінні – комплексі маркетингу), бути реальною або уявною. Інструментом реалізації стратегії диференціації є ринкове позиціонування.

Переваги стратегії за Ж.-Ж. Ламбеном:

- по відношенню до прямих конкурентів диференціація знижує ступінь замінності товару, посилює прихильність марці, зменшує чутливість до ціни і тим самим підвищує рентабельність;
- прихильність клієнтів послабляє їх тиск на фірму і перешкоджає приходу на ринок нових конкурентів;
- підвищена рентабельність збільшує стійкість до можливого зростання витрат в результаті дій сильного постачальника;
- відмітні властивості товару і завойована прихильність клієнтів захищають фірму і від товарів-замінників.

Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).

При веденні конкурентної боротьби з використанням цієї стратегії на ринку в першу чергу терплять фіаско фірми, що не здатні визначати потреби цільових ринків, оперативно реагувати на зміни в ринковому попиті, проводити ефективну політику маркетингових комунікацій, не мають необхідних навичок в області брендингу. Найважливішими здібностями, які повинна мати компанія, що приймає цю стратегію, є з генерування маркетингових ноу-хау, здійснення продуктових новацій.

Стратегія спеціалізації передбачає концентрацію на потребах одного цільового сегменту, без прагнення охопити увесь ринок. Мета тут полягає в задоволенні потреб вибраного цільового сегменту краще, ніж конкуренти. Така стратегія може спиратися як на диференціацію, так і на лідерство по витратах,

або і на те, і на інше, але тільки у рамках цільового сегменту. Проте низька ринкова доля у разі невдалої реалізації стратегії може істотно підірвати конкурентоспроможність компанії.

Таблиця 4.15 – Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Ключові конкурентоспроможні позиції відповідно до обраної альтернативи*	*Базова стратегія розвитку*
	Розробка програмного продукту, PR, просування бренду	Масовий маркетинг	Екстра-новий спосіб протидії всім видам SCA	Стратегія диференціації

Наступним кроком обрано стратегію конкурентної поведінки (таблиця 4.16).

Стратегія лідера

Залежно від міри сформованості товарного(галузевого) ринку, характеру конкурентної боротьби компанії-лідери обирають одну з трьох стратегій: розширення первинного попиту, оборонну або наступальну стратегію або ж застосувати демаркетинг або диверсифікацію.

Стратегія розширення первинного попиту доцільна у разі, якщо фірмі-лідерові недоцільно розмінюватися на боротьбу з невеликими конкурентами, вона може отримати велику економічну віддачу від розширення первинного рівня попиту. В цьому випадку компанія займається реалізацією заходів по формуванню попиту(навчанню споживачів користуванню товаром, формування регулярного попиту, збільшення разового споживання), також пропаганду нових напрямів застосувань існуючих товарів, виявлень нових груш споживачів. Розширюючи таким чином ринковий попит, лідер надає допомогу усім підприємствам, що «йдуть за ним», несучи при цьому основні фінансові витрати, проводячи найбільш революційні НДДКР. Така стратегія можлива тільки на початкових стадіях життєвого циклу товару, коли попит ще є

розширюваним, а взаємний тиск конкурентів ще невеликий. Інакше фірмі лідерові необхідно приймати оборонну або наступальну стратегію.

У міру зростання ринку, його становлення позиції компанії-новатора починають атакувати конкуренти-імітатори. В цьому випадку, компанія може вибрати оборонну стратегію, метою якої є захист власної ринкової долі. Оборона може бути:

- інновації з метою постановки технологічних бар'єрів для входу в ринок нових конкурентів, подальшого збільшення відриву від них;
- ліквідація ніш для проникнення конкурентів за допомогою розширення товарного асортименту, цінових парасольок, захоплення каналів збуту;
- ведення цінової війни і/або проведення масованої рекламної атаки.

Наступальна стратегія припускає збільшення своєї частки ринку. При цьому переслідувана мета полягає в подальшому підвищенні прибутковості роботи компанії на ринку за рахунок максимального використання ефекту масштабу. Проте, існує межа, при перевищенні якої подальше зростання частки ринку стає невигідним. Це або чисто економічна недоцільність відвойовування добре захищених часток, що сильно захищаються, у дрібніших виробників або ж попадання під дію антимонопольного законодавства.

Наступальна стратегія припускає активну інноваційну політику компанії. Вона постійно атакує власні ж досягнення, збільшуючи розрив між собою і основними конкурентами. Постійні техніко-економічні вдосконалення, модифікація розміру і форми упаковки, використання event- маркетингу – типові складові арсеналу фірм-лідерів.

Якщо фірма потрапляє під дію антимонопольного законодавства, вона може удатися до стратегії демаркетинга, що припускає скорочення своєї частки ринку, зниження рівня попиту на деяких сегментах за рахунок підвищення ціни. При цьому ставиться завдання недопущення на ці сегменти конкурентів, а

компенсація втрат прибутку через зменшення обсягів виробництва компенсується встановленням надвисоких цін.

Проте у більшості випадків найпривабливішою стратегією для компаній-лідерів є диверсифікація, що дозволяє використати переваги масштабу виробництва, know – how.

Стратегія виклику лідера

Стратегію виклику лідерові найчастіше вибирають компанії, які є другими, третіми на ринку, але бажають стати лідером ринку. Теоретично, ці компанії можуть прийняти два стратегічні рішення: атакувати лідера у боротьбі за частку ринку або ж йти за лідером.

Рішення атакувати лідера є досить ризикованим. Для його реалізації потрібні значні фінансові витрати, know – how, краще співвідношення «ціна-якість», переваги в системі розподілу і просування і т. д. У разі не реалізації цієї стратегії, компанія може бути відкинута на аутсайдерські позиції на досить довгий час. Тому реалізація цієї стратегії вимагає детального опрацювання по наступних напрямах:

- аналіз сильних і слабких сил своїх і фірми-лідера;
- виявлення можливих напрямів атаки;
- ревізія власних сил і ресурсів;
- аналіз можливих дій конкурентів і розробка методів захисту.

Залежно від цього компанія може вибрати одну з альтернативних стратегій: фронтальної або флангової атаки.

Фронтальна атака припускає атаку на сильні сторони конкурента. Така стратегія вимагає наявності у фірми значної переваги над тим, що атакує. У військовій стратегії це співвідношення зазвичай складає 3: 1. При цьому складно не лише стати першим, а мати можливості утримати першість в подальшому. Нового лідера атакуватиме не лише програвша фірма, але і треті, четверті в надії переділити ринок. В силу цього ця стратегія є найбільш

ризиковою і у разі невдачі відбувається « виснаження» компанії, що може привести до значного відкидання підприємства. У разі ж успіху компанія стає лідером ринку з усіма перевагами цієї позиції.

Флангова атака передбачає атаку на слабкі сторони фірми-лідера, наприклад, неосвоєні або погано відстежувані регіональні ринки або ринкові сегменти, ціну, значущий для споживача сервіс або показники якості продукції. Особливо б'є по лідерові цінова атака, оскільки, маючи велику ринкову частку, при зниженні ціни в абсолютному вираженні лідер терпить великі втрати, а недостатній приплив фінансових ресурсів відразу ж оголяє раніше приховані латентні слабкі місця компанії, може привести до системної кризи.

Стратегія наслідування лідеру

Компанії, що приймають слідування за лідером – це підприємства з невеликою часткою ринку, які вибирають адаптивну лінію поведінки на ринку, усвідомлюють своє місце на нім і йдуть у фарватері фірм-лідерів. Головна перевага такої стратегії – економія фінансових ресурсів, пов'язаних з необхідністю розширення товарного(галузевого) ринку, постійними інноваціями, витратами на утримання домінуючого положення.

Стратегія наслідування лідеру найчастіше має місце у випадку олігополії, коли кожен конкурент прагне уникнути боротьби, особливо цінової, а також у випадку, коли слабо виражений ефект масштабу, що не дозволяє отримати переваги від об'ємів продажів або ж він не грає істотної ролі. Стратегію наслідування лідеру приймають також фірми, які не змогли реалізувати стратегію виклику лідерові.

Компанії, що приймають таку стратегію, зазвичай випускають товари-імітатори, займаючи ринкову частку, яку з різних причин не можуть охопити фірми лідери. Вибір такої стратегії може також бути обумовлений також перевагою локалізації (краще знання ринку, налагоджені зв'язки з клієнтами тощо).

Для ефективної реалізації цієї стратегії компанії повинні задовольняти наступним основним умовам:

- систематичний аналіз сегментації ринку з метою виділення нових ринкових сегментів або таких, що незадовільно обслуговуються;
- ефективне використання НДДКР з метою вдосконалення технологічних процесів і незначних продуктових новацій;
- концентрація на прибутковості, а не на простому зростанні об'ємів продажів;
- постійний аналіз витрат на всіх стадіях виробництва і логістики;
- залишатися досить малим, щоб не бути досить цікавим для фірм-лідерів;
- сильний керівник, здатний не лише формулювати стратегію, але і тримати усю діяльність компанії під власним контролем.

Якщо врахувати, що лідерами ринку можуть бути лише декілька компаній, то ця стратегія є наймасовішою.

Стратегія заняття конкурентної ніші.

При прийнятті стратегії зайняття конкурентної ніші (інші назви – стратегія фахівця або нішера) компанія в якості цільового ринку вибирає один або декілька ринкових сегментів. Головна особливість – малий розмір сегментів/сегменту. Ця конкурентна стратегія являється похідною від такої базової стратегії компанії, як концентрація.

Ніша, для того, щоб вона була привабливою для компанії, повинна задовольняти таким умовам:

- бути досить прибутковою, щоб робити доцільним процес виробництва і обслуговування;
- залишатися стабільною упродовж тривалого проміжку часу;
- має бути добре захищеною, мати високі вхідні бар'єри;
- бути непривабливою для конкурентів;

- відповідати цілям і ресурсам компанії, її специфічним можливостям.

Головне завдання для компаній, що вибирають стратегію нішера або фахівця, – це постійна турбота про підтримку і розвиток своєї конкурентної переваги, формування лояльності і прихильності споживачів, підтримка вхідних бар'єрів.

Таблиця 4.16 – Визначення базової стратегії конкурентної поведінки

№ п/п	*Чи є проект «першопрохідцем» на ринку?*	*Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?*	*Чи буде компанія копіювати основні характеристики товару конкурента, і які?*	*Стратегія конкурентної поведінки*
	Ні	Забирати існуючих	Ні	Стратегія наслідування лідеру

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту (див. таблицю 4.5), а також в залежності від обраної базової стратегії розвитку (таблиця 4.15) та стратегії конкурентної поведінки (таблиця 4.16) розроблено стратегію позиціонування (таблиця 4.17), що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Позиціювання — це маркетингове забезпечення товарові бажаного місця на ринку і у свідомості потенційних покупців (образ). Позиція компанії чи продукту показує чим він унікальний УТП (унікальну торговельну пропозицію), чим відрізняється від конкурентів (відстройка від конкурентів), чим корисний споживачу.

З точки зору маркетингу товар являє собою сукупність відчутних (розмір, колір, маса, швидкість і т. п.) і невловимих (престижність, модність, сучасність і т. п.) властивостей.

Дослідження свідчать, якщо позиціювання здійснюється більше ніж за трьома ознаками, то воно є неефективним, оскільки не відкладається у свідомості споживача.

Результатом виконання підрозділу стала узгоджена система рішень щодо ринкової поведінки стартап-компанії, яка визначає напрями роботи стартап-компанії на ринку.

Таблиця 4.17 – Визначення стратегії позиціонування

№ п/п	*Вимоги до товару цільової аудиторії*	*Базова стратегія розвитку*	*Ключові конкурентоспроможні позиції власного стартап-проекту*	*Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)*
1	Невисока ціна, надійність	Позиціонування за показниками надійності	Присутність протидій SCA	Економічність, екологічність, ергономічність

4.5 Розроблення маркетингової програми стартап-проекту

Сформовано маркетингову концепцію товару, який отримає споживач. Для цього у таблиці 4.18 підсумовано результати попереднього аналізу конкурентоспроможності товару. Концепція товару - письмовий опис фізичних та інших характеристик товару, які сприймаються споживачем, і набору вигод, які він обіцяє певній групі споживачів.

Таблиця 4.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)*
	Протидія методам аналізу по стороннім каналам	Забезпечення надійності особистих даних користувачів	Рішення є надійним
	Ціна	Низька ціна	Нижча ціна.

Розроблено трирівневу маркетингову модель товару: уточнюється ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання (таблиця 4.19).

1-й рівень

При формуванні задуму товару вирішується питання щодо того, засобом вирішення якої потреби і / або проблеми буде даний товар, яка його основна вигода. Дане питання безпосередньо пов'язаний з формуванням технічного завдання в процесі розробки конструкторської документації на виріб.

2-й рівень

Цей рівень являє рішення того, як буде реалізований товар в реальному/ включає в себе якість, властивості, дизайн, упаковку, ціну.

3-й рівень

Товар з підкріпленням (супроводом) - додаткові послуги та переваги для споживача, що створюються на основі товару за задумом і товару в реальному виконанні (гарантії якості , доставка, умови оплати та ін).

Таблиця 4.19 – Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>I. Товар за задумом</td><td colspan="3">Товар дозволяє шифрувати дані алгоритмом RSA, забезпечує надійність та протидію SCAатакам.</td></tr>
<tr><td rowspan="5">II. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх /Тл/Е/Ор</td></tr>
<tr><td>1. Якість
2. Простота у використанні
3. Низька ціна</td><td>-</td><td>-</td></tr>
<tr><td colspan="3">Якість: згідно до стандарту ISO 4444 буде проведено тестування</td></tr>
<tr><td colspan="3">Пакування у мікроконтролер TM4C1294NCDP</td></tr>
<tr><td colspan="3">Марка (власна): E-Secure</td></tr>
<tr><td rowspan="2">III. Товар із підкріпленням</td><td colspan="3">До продажу: базова версія</td></tr>
<tr><td colspan="3">Після продажу: постійне вдосконалення протидій</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: ноу-хау</td></tr>
</table>

Після формування маркетингової моделі товару слід відмітити, що проект буде захищено від копіювання за допомогою ноу-хау.

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів (таблиця 4.20). Аналіз проведено експертним методом.

Таблиця 4.20 – Визначення меж встановлення ціни

№ п/п	*Рівень цін на товари-замінники*	*Рівень цін на товари-аналоги*	*Рівень доходів цільової групи споживачів*	*Верхня та нижня межі встановлення ціни на товар/послугу*
	3-4$	3-4$	10 000 000$	2-2.3 $

Наступним кроком є визначення оптимальної системи збуту, в межах якого було прийняте рішення (таблиця 4.21):

- проводити збут власними силами і залучати сторонніх посередників.
- користуватися однорівневим каналом збуту;

Таблиця 4.21 – Формування системи збуту

№ п/п	*Специфіка закупівельної поведінки цільових клієнтів*	*Функції збуту, які має виконувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*
	Оптом	Оптова торгівля	Однорівневий	Власні сили та через посередників

Останньою складовою маркетингової програми є розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів (таблиця 4.22).

Таблиця 4.22 – Концепція маркетингових комунікацій

№ п/п	*Специфіка поведінки цільових клієнтів*	*Канали комунікацій, якими користуються цільові клієнти*	*Ключові позиції, обрані для позиціонування*	*Завдання рекламного повідомлення*	*Концепція рекламного звернення*
	Клієнти обиратимуть товар з у більш рентабельних фірм на ринку.	Внутрішні переписки.	Ціна, надійність	Показати переваги продукту, низьку ціну, надійність.	Інтернет реклама.

Результатом підрозділу стала ринкова (маркетингова) програма, що включає в себе концепції товару, збуту, просування та попередній аналіз можливостей ціноутворення, спирається на цінності та потреби потенційних клієнтів, конкурентні переваги ідеї, стан та динаміку ринкового середовища, в межах якого впроваджено проект, та відповідну обрану альтернативу ринкової поведінки.

Висновки

В даному розділі було проведено аналіз програмного продукту у якості стартап проекту. Можна зазначити що у проекту низьку можливість до комерціалізації, адже він в першу чергу зацікавить великі компанії, які займаються розробкою подібних приладів. Він не є універсальним, а тому може зацікавити лише як підхід до вирішення проблем зі сторонніми каналами, а не як готовий товар.

На ринку наявна монополістична конкуренція, існує декілька фірм-конкурентів, тому вихід на нього не буде легким. Проект є конкурентоспроможним лише завдяки, в першу чергу, своїй високій надійності. Також проект включає витрати на мікроконртолери, де ідея буде реалізована.

Для впровадження ринкової реалізації проекту слід обрати альтернативу, яка передбачає розробку програмного продукту, а потім якісну рекламу та PR,

сконцентровану навколо позитивних характеристиках даного програмного продукту, таких як низька ціна, надійність, безпека і т.д.

З огляду на проведений аналіз, можна чітко сказати, що подальша імплементація проекту не є доцільною, адже він може знайти свою цільову аудиторію та зайняти місце на ринку дуже багатьма зусиллями й скоріше не буде прибутковим.

ВИСНОВОК

Конфіденційність даних у наш час вимагає досить великий спектр захист для безпечного зберігання та обробки. Широко застосовуються криптографічні алгоритми, такі як RSA та AES. Спектр можливих атак на дані алгоритм розширюється, і хоча вони обидва є криптостійкими до математичного аналізу, їх реалізація може зовсім не гарантувати безпеку.

У даній роботі розглянуто можливі спектри атак на алгоритм RSA, що зосереджуються на інформації по стороннім каналам. Це дуже широкий напрямок аналізу сигналів, що можуть бути отримані та характеризувати роботи будь-якого електронного пристрою.

Аналіз сучасних, існуючих методів аналізу криптосистем по стороннім каналам показав, що загроза дійсно існує. Це не раз підтверджувалось на багатьох конференціях та нажаль не мало однозначного виходу з ситуації. Особливості кожної системи настільки індивідуальні, що вироблення одного одначно надійного підходи до впровадження безпеки в алгоритм RSA чи інший крипто модуль – неможливо.

Дослідження методів протидій аналізу інформації, яку несуть сторонні канали показало, що доцільним є дослідження середи реалізації криптосистеми при виборі методів, які будуть впроваджуватись задля підвищення надійності алгоритму. Серед безперечно корисних підходів виділяються ті, що використовують апаратні методи захисту. Зміна частоти роботи процесора чи додавання преривань, може сильно змінити сигнал, так що його форма буду не відновлюваною.

Для аналізу роботи криптосистему було розроблено пристрій, що збирає дані та обробляє для подальшого аналізу. Він являє собою конвертор заміряного каналового сигналу, що дискретизує його, підсилює та передаю через USB конвертор на комп’ютер, де він зберігається у вигляді одно канального файлу.

Використовуючи програмні засоби, надалі було проаналізовано отримані заміри. Під час аналізу з використанням методів цифрової обробки сигналів, а саме розклад у спектр неперіодичного сигналу за допомогою віконного перетворення Фур'є, сигнал був досліджений на інформативні процеси, які свідчать про роботу криптосистеми.

За результатами дослідження був зроблений висновок, про доцільність використання методів протидії аналізу криптосистем. Апаратне приховання та рандомізація у даному випадку показали великий рівень надійності, хоча не приховували активність криптосистеми.

Результатами цієї роботи є рекомендації, щодо використання методів протидії крипто аналізу по стороннім каналам для підвищення надійності криптосистеми, зменшення інформативності сторонніх каналів, а також забезпечення конфіденційності приватним даним.

Кожна фірма, що цінує безпеку та якість своїх продуктів, при реалізації криптосистем повинна зосередити увагу на кореляції написаного коду, з її відкликом у споживанні ресурсів. Конфіденційність завжди повинна бути пріоритетом, і криптосистема має бути надійною в усіх випадках. Недосконалості системи завжди будуть нести багато інформації про внутрішню роботу, а отже питання інформативності сторонніх каналів та шляхи його зменшення завжди будуть темою для дискусій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Євчук О. В. Цифрова обробка сигналів : конспект лекцій, Івано-Франківськ : ІФНТУНГ, 2010, 135 с.
2. Сергиенко А.Б. Цифровая обработка сигналов, СПб.: Питер, 2003, 604с.
3. Бабак В.П., Хандецький В.С., Шрюфер Е.К. Обробка сигналів: Підручник, Либідь, 1996, 392с.
4. Айфичер Э., Джефрис Б. Цифровая обработка сигналов: практический поход 2-е.,М:Вильямс, 2004, 992с.
5. Сойфер В.А., Сергеев В.В. и др. Теоретические основы цифровой обработки изображений, Самара, 2000, 256с.
6. Марпл С.Л. Цифровой спектральный анализ и его приложения, М:Мир, 1990.
7. F. Hlawatsch and F. Auger. Time-Frequency Analysis, John Wiley & Sons, 2008, 440p.
8. Аліасинг.: [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Аліасинг. - Дата доступу: 28.04.2017
9. Спектральный анализ на ограниченном интервале времени. Оконные функции. [Электронный ресурс]. – Режим доступу: http://www.dsplib.ru/content/win/win.html. - Дата доступу: 28.04.2017
10. Evgeny Milanov. The RSA Algorithm, 2009 [Електронний ресурс]. – Режим доступу: https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf .- Дата доступу: 05.05.2017
11. G.N. Shinde, H.S. Fadewar. Faster RSA Algorithm for Decryption Using Chinese Remainder Theorem, [Електронний ресурс]. – Режим доступу: http://www.techscience.com/doi/10.3970/icces.2008.005.255.pdf .- Дата доступу: 05.05.2017
12. Johann Großschadl. The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip, Graz University of Technology, Institute for

Applied Information Processing and Communications, Inffeldgasse 16a, A–8010 Graz, Austria

13. Joye, M. and F. Olivier. Side-channel analysis, Encyclopedia of Cryptography and Security, 571–576, 2005.
14. Peter Gutmann, David Naccache, Charles C. Palmer. Side Channel attacks on Cryptographic software, Copublished by the IEEE computer and reliability societies 1540-7993, November 2009
15. YongBin Zhou, DengGuo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China
16. Kocher, Paul C. Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks, Advances in Cryptology, CRYPTO ’95: 15th Annual International Cryptology Conference, 27–31. Springer-Verlag, 1995.
17. Dhem, J.F., F. Koeune, P.A. Leroux, P. Mestr´ e, J.J. Quisquater, and J.L. Willems. A practical implementation of the timing attack, Smart Card Research and Applications, 167–182. Springer, 2000.
18. Schindler, Werner. A Timing Attack against RSA with the Chinese Remainder Theorem, Cryptographic Hardware and Embedded Systems CHES 2000, volume 1965 of Lecture Notes in Computer Science, 109–124. Springer Berlin Heidelberg, 2000.
19. Marc Joye, Michael Tunstall. Fault Analysis in Cryptography, Springer-Verlag Berlin Heidelberg, 2012
20. Stefan Mangard, Elisabeth Oswald, Thomas Popp. Power Analysis Attacks: Revealing the Secrets of Smart Cards, 2007 Springer Science+Business Media, LLC
21. Christophe Clavier, Benoit Feix, Georges Gagnerot, Georges Gagnerot , Vincent Verneuil. Horizontal Correlation Analysis on Exponentiation, 2010, XLIM-CNRS, Universite de Limoges, Limoges, France

22. D.Chaum. Blind Signatures for untraceable payments, CRYPTO’82, pp.199-203,1983.
23. D.Chaum. Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms, AUSCRYPT’90, LNCS 453, pp.246-264,1990.
24. Ei Biham, Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems
25. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis
26. Thomas S. Messerges, Ezzy A. Dabbish, Robert H. Sloan. Investigation of Power Analysis Attack on Smartcards
27. Hagai Bar-El. Introduction to Side Channel attacks, Discretix Technologies Ltd.
28. Josh Jaffe and Pankaj Rohatgi.Efficient side-hannel testing for public key algorithms:RSAcase study, Cryptography Research Inc,Marc Witteman, Riscure
29. Joe Grand. Tools of the Hardware Hacking Trade, RSA Conference 2015, San Francisco
30. Junrong Liu, Yu Yu, Francois-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, Xinjun Xie. Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China
31. Brier E., Clavier C., Olivier F. Correlation power analysis with a leakage model, 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), pp. 16-29 (2004)
32. B. Preneel, A. Biryukov, C. De Canni`ere, S. B. Ors, E. Oswald, B. Van Rompay, L. Granboulan, E. Dottax, G. Martinet, S. Murphy, A. Dent, R. Shipsey, C. Swart, J. White, M. Dichtl, S. Pyka, M. Schafheutle, P. Serf, E. Biham, E. Barkan, Y. Braziler, O. Dunkelman, V. Furman, D. Kenigsberg, J. Stolin, J-J. Quisquater, M. Ciet, F. Sica, H. Raddum, L. Knudsen, M. Parker.

Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, 2004

33. Job de Haas. Side Channel Analysis and Embedded Systems Impact and Countermeasures, Black Hat Europe, 2008
34. Siddika Berna Ors Yalcin. Side-channel Attacks On Hardware Implementations Of Cryptographic Algorithms, Istanbul Technical University, Department of Electronics and Communication Engineering
35. A. Shamir. Method and apparatus for protecting public key schemes from timing and fault attacks, US patent number 5,991,415, November 1999.
36. S. B. Ors, E. Oswald, and B. Preneel. Power-analysis attacks on an FPGA - first experimental results, Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), volume 2779 of Lecture Notes in Computer Science, pages 35-50, Cologne, Germany, September 7-10 2003. Springer-Verlag.
37. F.-X. Standaert, C. Archambeau. Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages, UCL Crypto Group, Universit´e catholique de Louvain, Centre for Computational Statistics and Machine Learning, University College London
38. W. Schindler, K. Lemke, C. Paar. A Stochastic Model for Differential Side-Channel Cryptanalysis, CHES 2005, Lecture Notes in Computer Science, vol 3659, pp 30-46, Edinburgh, Scotland, September 2005.
39. Pierre-alain Fouque, Sebastien Kunz-Jacques, Gwenaelle Martinet, Frederic Muller, Frederic Valette. Power Attack on Small RSA Public Exponent, DCSSI Crypto Lab, France
40. Chujiao Ma and Z. Jerry Shi. Side channel attack: Power Analysis, Computer Science and Engineering, University of Connecticut
41. Zdenek Martinasek, Vaclav Zeman, Krisztina Trasy. Simple Electromagnetic Analysis in Cryptography, 2007